1 集　　合

集合是数学中最基本的概念，它已深入到各种科学和技术领域中，特别是应用于数学的各个分支中．本章的内容是在高中数学课所介绍的基础上略有提高，引入了幂集、积集概念以及计算机科学中常用的集合的归纳定义．

1.1 集合的基本概念

1.1.1 集　　合

集合是一些对象的总体．总体中的对象称之为集合的元素或成员．给定任意一个对象 x 以及集合 S，如果 x 是集合 S 的一个元素，我们将写成 $x \in S$．如果 x 不是集合 S 的一个元素，则写成 $x \notin S$．

习惯上称之为集合的东西，通常在数学上是可以接受的．例如：

1° “小于 4 的非负整数集合”是由四个元素组成的集合．这四个元素分别是 0，1，2，3．

2° “全体活着的中国人”是个集合．集合中元素的个数很多，但是有限的．由于生死的变化，要列出这个集合的成员是困难的．这种困难是实践上的，不是理论上的．

3° “大于等于 3 的整数集合”是个有无限多个元素的集合．要判断一个整数是否是它的元素很容易．

4° “在具有无限存贮量的计算机上，运行足够长的时间之后能停止运行的所有 Algol 60 程序组成了一个无限集合”．可计算

理论已经证明，判断任意程序是否是这个集合的元素的算法是不存在的。从而这个集合是不可判定的。

5° “全体大于 0，小于 1 的整数集合”。在这个集合中没有任何元素，我们称它为空集，并记为 $\varnothing$。

集合是以它的元素来表征的。一个有有限多个元素的集合可以用列出它的全部元素的方法来说明。这些元素用括号括起来，并且元素之间用逗号分开。一般集合用大写字母表示，集合元素用小写字母表示。当集合 A 中有有限多个元素时，用 $|A|$ 表示集合中的元素个数．特别对于空集 $\varnothing$，$|\varnothing|=0$。例如：

1° $A=\{a, b, c\}$，a，b，c 是集合 A 的元素，$|A|=3$。

2° $B=\{0, 2, 4, 6, 8\}$，B 是小于 10 的非负偶数集合。$|B|=5$。

集合，特别是有无限多个元素的集合，通常用指出集合中元素性质的方法来说明。例如，记 $\mathbf{Z}$ 是全体整数集合，

1° 全体偶数集合为$\{x \mid \exists y \in \mathbf{Z}, x=2y\}$。

2° 大于 10 的整数集合$\{x \mid x \in \mathbf{Z}$ 且 $x>10\}$。

3° 有理数集合 $\mathbf{Q}=\{x/y \mid x, y \in \mathbf{Z}$ 且 $y \neq 0\}$。

1.1.2 集合的相等

同一个集合可以有不同的表示法。例如，$A=\{-1, 1\}$，$B=\{x \mid x \in \mathbf{Z}, x^2=1\}$，$C=\{x \mid x \in \mathbf{R}, |x|=1\}$，其中 $\mathbf{R}$ 表示全体实数集合。这就产生了一个问题，即如何判断两个集合是同一个集合。

定义 1.1 **给了两个集合 A 和 B，如果集合 A 中的每个元素都是集合 B 中的元素，反过来集合 B 的每个元素也都是集合 A 中的元素，那么称集合 A 与集合 B 相等，并记为 $A=B$。**

用这个定义可直接验证上面的集合 A，B，C 是相等的集合，$A=B=C$。

定理 1.1 **A，B，C 是任意集合，集合间的相等关系满足**

1° **自反性** $A=A$。

2° **对称性** 若 $A=B$，则 $B=A$。

3° **传递性** 若 $A=B$，$B=C$，则 $A=C$。

证明 在定义1.1中，将 B 改成 A 以后显然成立，它说明 $A=A$。又在定义1.1中，先说后一句话，再说前一句话，也就是说集合 B 的每个元素都是集合 A 中的元素，反过来集合 A 的每个元素也都是集合 A 中的元素，其意思与原来完全相同，所以当 $A=B$ 时，必有 $B=A$。

下面证明传递性。已知 $A=B$，对于任何 $x\in A$，必有 $x\in B$。又由 $B=C$，从 $x\in B$ 推出 $x\in C$。反过来，由 $A=B$，$B=C$ 及相等关系的对称性推出 $B=A$，$C=B$。对于任何 $x\in C$，由于 $C=B$，必有 $x\in B$。又由 $B=A$ 从 $x\in B$ 推出 $x\in A$。对照定义1.1知 $A=C$。

1.1.3 集合的包含

集合的相等与包含是集合间的两种最基本的关系。现在定义两个集合的包含关系。

定义1.2 **A 和 B 是两个集合。如果集合 A 中的每个元素都是集合 B 中的元素，我们称集合 B 包含集合 A，而集合 A 叫做集合 B 的一个子集，表示成 $B\supseteq A$ 或 $A\subseteq B$。**

如果集合 B 包含集合 A，并且至少有一个元素属于集合 B 而不属于集合 A，我们称集合 B 真包含集合 A，而集合 A 叫做集合 B 的一个真子集。

例如，偶数集合是整数集合的真子集。集合 $\{1, 2, 3, 4\}$ 是集合 $\{x|x\in Z 且 0<x<5\}$ 的子集，但不是真子集。

定理1.2 **A, B, C 是任意集合。集合间的包含关系满足**

1° **自反性** $A\subseteq A$。

2° **反对称性** 若 $A\subseteq B$ 且 $B\subseteq A$，则 $A=B$。

3° **传递性** 若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$。

证明 1°，3°的证明留作习题。这里只证 2°。

若 $A\subseteq B$ 且 $B\subseteq A$，由集合包含的定义知集合 A 中的每个元素都是集合 B 中的元素，并且集合 B 中的每个元素都是集合 A 中的元素。这正是集合 A 与集合 B 相等的定义，从而得出 $A=B$。

定理 1.3 对于任何集合 A，$\varnothing\subseteq A$。

证明 用反证法。假设空集$\varnothing$不是某个集合 A 的子集，那么至少有一个元素 x，$x\in\varnothing$ 且 $x\notin A$。而 $\varnothing$ 是空集，它没有任何元素，即对任何 x 必有 $x\notin\varnothing$。产生矛盾，故不可。由此得出 $\varnothing$ 是任何集合 A 的子集。

由定理 1.3 知空集 $\varnothing$ 是唯一的。这是因为假若 $\varnothing_1$ 和 $\varnothing_2$ 都是空集。因为 $\varnothing_1$ 是空集，得出 $\varnothing_1\subseteq\varnothing_2$。因为 $\varnothing_2$ 是空集，得出 $\varnothing_2\subseteq\varnothing_1$。由集合包含关系的反对称性知 $\varnothing_1=\varnothing_2$。

在研究一个特定问题时，假设有一个足够大的集合使一切集合都包含在它之中。这个足够大的集合称之为万有集合，并记为 U。对于任意集合 A 均有 $A\subseteq U$。

1.1.4 幂　　集

A，B，…是集合，把它们放在一起构成一个新的集合$\{A, B, \cdots\}$。这种集合以集合作为元素称为集族。集族通常用花写字母 $\mathscr{A}$，$\mathscr{B}$，…表示。

一个集合的全部子集构成的集族叫做该集合的幂集。若 $A=\{a, b, c\}$，A 的幂集 $\mathscr{P}(A)$是有 8 个元素的集族。

$\mathscr{P}(A)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c,\}\}$。

定理 1.4 A 是有限集合，$|\mathscr{P}(A)|=2^{|A|}$。

证明 A 是有限集合，$|A|=n$。A 的 i 元子集的个数就是从 n 个元素中选取 i 个不同元素的方法数 $C_n^i\left(=\dfrac{n!}{i!(n-i)!}\right)$，这里 i 可以取 0，1，…，n 这 $n+1$ 个值。

$$|\mathscr{P}(A)|=C_n^0+C_n^1+\cdots+C_n^n.$$

在二项式定理

$$(x+y)^n=C_n^0x^ny^0+C_n^1x^{n-1}y+\cdots+C_n^nx^0y^n$$

中，令 $x=y=1$，于是有 $2^n=C_n^0+C_n^1+\cdots+C_n^n$。从而 $|\mathscr{P}(A)|=2^n=2^{|A|}$。

1.1.5 积　　集

定义 1.3　对于正整数 n，有序 n 数组 $(a_1,a_2,\cdots,a_n)$ 是以 a_i 为第 i 个分量的 n 个对象的序列。

两个有序 n 数组是相等的，当且仅当它们的每个分量都是相等的。

定义 1.4　n 个集合 $A_1, A_2, \cdots A_n$ 的积集 $A_1\times A_2\times\cdots\times A_n$ 是由全体有序 n 数组 $(a_1, a_2, \cdots, a_n)$ 构成的集合，其中 $a_i\in A_i$，$1\leqslant i\leqslant n$。

特别地，若 $A_1=A_2=\cdots=A_n=A$ 时，记 $A_1\times A_2\times\cdots\times A_n$ 为 A^n。

例如，$A=\{1, 2\}$，$B=\{m, n\}$，$C=\{0\}$．$D=\varnothing$，那么

$$A\times B=\{(1, m), (1, n), (2, m), (2, n)\},$$

$$A\times C=\{(1, 0), (2, 0)\},$$

$$C\times A=\{(0, 1), (0, 2)\},$$

$$A\times D=\varnothing.$$

注意，这里 $A\times C\neq C\times A$。

定理 1.5　A, B 是两个有限集合，$|A\times B|=|A|\cdot|B|$。

证明　从集合 A 中任取一个元素 a 作为第一分量，从集合 B 中任取一个元素 b 作为第二分量构成的有序 2 数组 (a, b) 是 $A\times B$ 的一个元素。a 与 b 的不同取法构成不同的有序 2 数组。从集合 A 中选取一个元素有 $|A|$ 种方法，从集合 B 中选取一个元素有 $|B|$ 种方法。它们可以构成 $|A|\cdot|B|$ 个不同的 2 数组。于是 $|A\times B|=|A|\cdot|B|$。

同理可以证明 $|A_1\times A_2\times\cdots\times A_n|=|A_1|\cdot|A_2|\cdot\cdots\cdot|A_n|$。

1.2 集合的运算

我们在前一节谈到集合间的一些联系，如包含，子集等，各种不同集合的进一步联系是通过集合上的各种运算显示出来的。

定义 1.5 集合 A 与 B 的并，交，差集 $A\cup B$，$A\cap B$，$A-B$ 分别为

$$A\cup B=\{x|x\in A \text{ 或 } x\in B\},$$
$$A\cap B=\{x|x\in A \text{ 且 } x\in B\},$$
$$A-B=\{x|x\in A \text{ 且 } x\notin B\}.$$

由定义看出 $A\cup B$ 是由或是在集合 A 中，或是在集合 B 中的元素组成的。$A\cap B$ 是由集合 A 和集合 B 的公共元素组成的。$A-B$ 是由在集合 A 中且不在集合 B 中的元素组成的。若取 A 为万有集合 U，$U-B$ 称为集合 B 的补集，并记为 $\bar{B}$。不难看出

$$\bar{B}=\{x|x\in U \text{ 且 } x\notin B\}=\{x|x\notin B\}.$$

例如，$A=\{0,1,2\}$，$B=\{1,2,3\}$，$U=\{x|x\in Z \text{ 且 } x\geqslant 0\}$。

$A\cup B=\{0,1,2,3\}$，

$A\cap B=\{1,2\}$，

$A-B=\{0\}$，$B-A=\{3\}$。

$\bar{A}=U-A=\{x|x\in Z \text{ 且 } x\geqslant 3\}$。

定理 1.6 对于任意集合 A，$A\cup\bar{A}=U$，$A\cap\bar{A}=\varnothing$。

证明 由并与交运算的定义

$A\cup\bar{A}=\{x|x\in A \text{ 或 } x\in\bar{A}\}=\{x|x\in A \text{ 或 } x\notin A\}=U$。

$A\cap\bar{A}=\{x|x\in A \text{ 且 } x\in\bar{A}\}=\{x|x\in A \text{ 且 } x\notin A\}=\varnothing$。

例 1 证明 $\bar{A}\subseteq\bar{B}$ 当且仅当 $B\subseteq A$。

证明 用反证法证明必要性。假设 $B\subseteq A$ 不成立，那么至少存在一个元素 $x_0\in B$ 且 $x_0\notin A$，从而 $x_0\in\bar{A}$。另一方面 $x_0\in B$，故 $x_0\notin\bar{B}$。这就是说，至少存在一个元素 x_0，使 $x_0\in\bar{A}$ 且 $x_0\notin\bar{B}$，与 $\bar{A}\subseteq\bar{B}$ 相矛盾，故不可。于是仅当 $B\subseteq A$ 时有 $\bar{A}\subseteq\bar{B}$。

可用类似的方法证明充分性。

例 2 证明 $\overline{A\cap B}=\overline{A}\cup\overline{B}$。

证明 证明的思路是先证明 $\overline{A\cap B}\subseteq\overline{A}\cup\overline{B}$，再证明 $\overline{A}\cup\overline{B}\subseteq\overline{A\cap B}$。利用集合间包含关系的反对称性得到 $\overline{A\cap B}=\overline{A}\cup\overline{B}$。

下面我们先证 $\overline{A\cap B}\subseteq\overline{A}\cup\overline{B}$：

任取 $x\in\overline{A\cap B}$，由补运算的定义知 $x\notin A\cap B$，即 $x\in A$ 与 $x\in B$ 不能同时成立。由此得出 $x\notin A$ 或 $x\notin B$。再由集合并运算的定义知 $x\in\overline{A}\cup\overline{B}$。这里 x 是 $\overline{A\cap B}$ 的任意元素，故 $\overline{A\cap B}\subseteq\overline{A}\cup\overline{B}$。

再证 $\overline{A}\cup\overline{B}\subseteq\overline{A\cap B}$：

任取 $x\in\overline{A}\cup\overline{B}$，由并运算的定义知 $x\in\overline{A}$ 或 $x\in\overline{B}$。因 $A\cap B\subseteq A$，从上例知 $\overline{A}\subseteq\overline{A\cap B}$。当 $x\in\overline{A}$ 时，必有 $x\in\overline{A\cap B}$。同样因 $A\cap B\subseteq B$，从上例知 $\overline{B}\subseteq\overline{A\cap B}$。当 $x\in\overline{B}$ 时，必有 $x\in\overline{A\cap B}$。综上分析知 $\overline{A}\cup\overline{B}$ 的每个元素都是 $\overline{A\cap B}$ 的元素，即 $\overline{A}\cup\overline{B}\subseteq\overline{A\cap B}$。**证毕**

定理 1.7 对任意集合 A, B, C 下面等式成立：

1° $A\cup B=B\cup A$，$A\cap B=B\cap A$。

2° $A\cup(B\cup C)=(A\cup B)\cup C$，$A\cap(B\cap C)=(A\cap B)\cap C$。

3° $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$，

$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$。

4° $A\cup\varnothing=A$，$A\cap U=A$。

5° $A\cup\overline{A}=U$，$A\cap\overline{A}=\varnothing$。

证明 5°已在定理 1.6 中证明。其余的均可由集合并，交运算的定义直接证明。

定理 1.8 下面三个关于集合 A 和 B 的命题是相互等价的。

1° $A\subseteq B$，

2° $A\cup B=B$，

3° $A\cap B=A$。

证明 我们的证明方法是通过证明 $1^\circ\Rightarrow2^\circ\Rightarrow3^\circ\Rightarrow1^\circ$ 来说明它们是等价的。

首先证明 $1^\circ\Rightarrow2^\circ$：

已知 $A\subseteq B$，A 的每个元素都是 B 中的元素，从集合并运算的定义知

$$A\cup B=\{x|x\in A \text{ 或 } x\in B\}=\{x|x\in B\}=B.$$

再证明 $2^\circ\Rightarrow3^\circ$：

已知 $A\cup B=B$，等式两边同时与 A 求交仍然相等，然后再定理 1.7 中的诸性质

$$\begin{aligned}
A\cap B&=A\cap(A\cup B)\\
&=(A\cup\varnothing)\cap(A\cup B) && 4^\circ\\
&=A\cup(\varnothing\cap B) && 3^\circ\\
&=A\cup((\varnothing\cap B)\cup\varnothing) && 4^\circ\\
&=A\cup((B\cap\varnothing)\cup(B\cap\bar{B})) && 1^\circ,\ 5^\circ\\
&=A\cup(B\cap(\varnothing\cup\bar{B})) && 3^\circ\\
&=A\cup(B\cap\bar{B}) && 1^\circ,\ 4^\circ\\
&=A\cup\varnothing && 5^\circ\\
&=A. && 4^\circ
\end{aligned}$$

最后证明 $3^\circ\Rightarrow1^\circ$：

已知 $A\cap B=A$，任取 $x\in A\cap B$，由集合交运算的定义知 $x\in A$ 且 $x\in B$，特别注意到 $x\in B$. 由 x 的任意性，得到 $A\cap B\subseteq B$。将 $A\cap B=A$ 代入即是所求的结果 $A\subseteq B$。

对集合的运算可以用 Venn 图直观地表示。在图 1 中用矩形表示万有集合 U，圆表示集合 A，B，C。

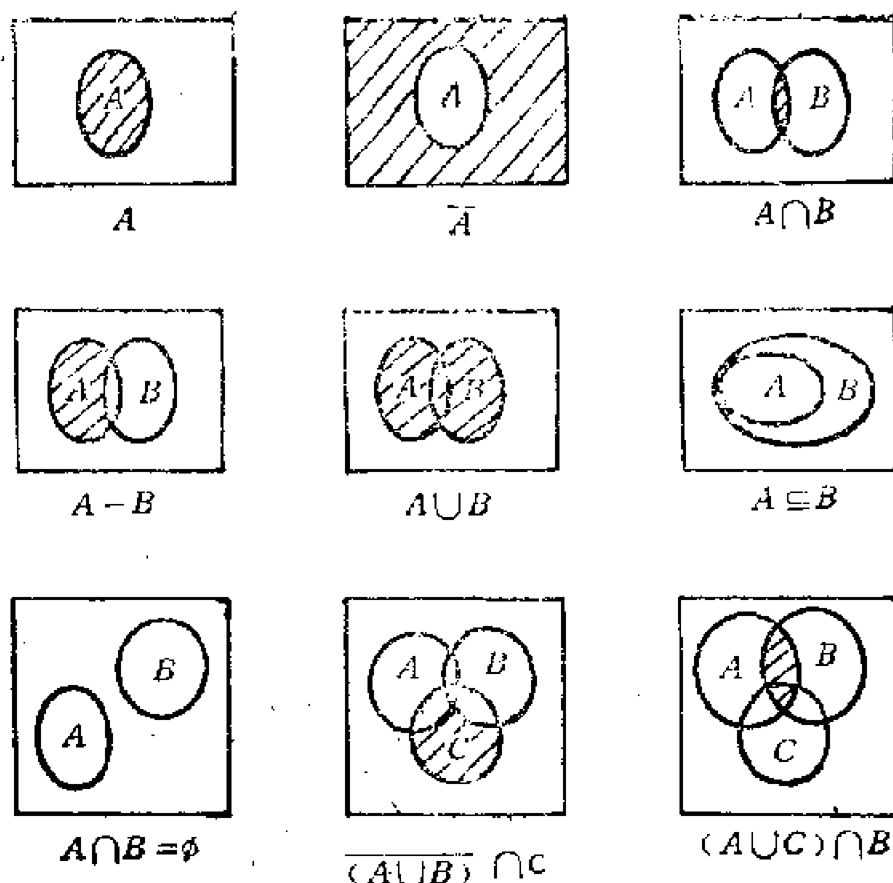


图 1 Venn 图

1.3 集合的归纳定义

前面谈到有限集合可以用列出集合元素的方法，也可以用刻划集合元素性质的方法来表述。但是用集合元素来定义集合，特别是无限集合，不总是很方便的。例如 pascal 程序集合，自然数集合等等。对这样的集合通常自然地采用归纳定义。

集合的归纳定义是由基础语句，归纳语句，和终结语句三个部分组成的。

先看个例子。非负偶整数集合 E 可以定义为

$$E=\{x|x\in \mathrm{Z},\ x\geqslant 0 \text{ 且 } \exists y\in \mathrm{Z},\text{ 使 } x=2y\}。$$

它也可以归纳定义如下：

1° （基础语句）$0\in E$，

2° （归纳语句）结果 $n \in E$，则 $n+2 \in E$。

3° （终结语句）除了有限多次使用 1°，2°产生的整数之外再也没有其它元素属于 E。

在这个例子中，我们可以看出：基础语句为该集合提供了基本建筑块。这些基本块应该尽可能地少。归纳语句指出如何从集合已有元素构造出其它元素。构造方法要简单可行。终结语句表述构造方法的完备性，即除掉基础语句给出的元素外，集合的每个元素都能用归纳语句提供的方法构造出来，并且该集合的全体元素就是有限次使用基础语句和归纳语句所得到的全部元素。

在计算机科学中符号行起着重要作用，在行文编辑程序、处理代数公式程序以及定理证明程序中，对符号行的运算是核心。字母表是由有限多个符号组成的集合，记为 Σ。从 Σ 中选取有限个符号排成一行称为字母表 Σ 上的一个行。令 $\Sigma=\{a_1, a_2, \cdots, a_n\}$，$x=a_{i_1}a_{i_2}\cdots a_{i_k}$，其中 $a_{i_1}, a_{i_2}, \cdots, a_{i_k} \in \Sigma$，那么称 x 是 Σ 上长为 k 的行。特别地，称长为 0 的行为空行，记作 λ。现有 Σ 上的两个行 $x=a_{i_1}a_{i_2}\cdots a_{i_k}$，$y=b_{j_1}b_{j_2}\cdots b_{j_l}$，其中 $a_{i_1}, a_{i_2}, \cdots, a_{i_k}, b_{j_1}, b_{j_2}, \cdots, b_{j_l} \in \Sigma$。行 x 与行 y 的连接是行 xy

$$xy=a_{i_1}a_{i_2}\cdots a_{i_k}b_{j_1}b_{j_2}\cdots b_{j_l},$$

它是 Σ 上长为 $k+l$ 的行。一般地，行的连接运算不满足交换律。

特别地，$x\lambda=\lambda x=x$，即任何行与空行相连接，则保持不变。

下面归纳定义两个常用的集合 Σ^+ 和 Σ^*。

定义 1.6　字母表 Σ 上所有非空行的集合 Σ^+ 定义如下：

1° （基础语句）如果 $a \in \Sigma$，则 $a \in \Sigma^+$。

2° （归纳语句）如果 $x \in \Sigma^+$ 且 $a \in \Sigma$，则 a 与行 x 的连接 $ax \in \Sigma^+$。

3° （终结语句）集合 Σ^+ 只包含有限次使用 1°，2° 所得到的那些行。

集合 Σ^+ 包括长为 1，2，…的行，它是一个无限集合。特别要指出的是，在 Σ^+ 中的每一个元素都是由有限多个符号组成的行。

例如 $\Sigma=\{a, b\}$，那么

$$\Sigma^+=\{a, b, aa, ab, ba, bb, aaa, aab, \cdots\}.$$

定义 1.7 Σ **是字母表，**Σ **上所有行的集合** Σ^* **定义如下：**

1° （基础语句）空行 $\lambda\in\Sigma^*$。

2° （归纳语句）如果 $x\in\Sigma^*$ 且 $a\in\Sigma$，则 a 与行 x 的连接 $ax\in\Sigma^*$。

3° （终结语句）除了有限次使用 1°，2° 构造的行以外，Σ^* 再没有其它元素。

例如 $\Sigma=\{a,b\}$，那么

$$\Sigma^*=\{\lambda, a, b, aa, ab, ba, bb, aaa, aab, \cdots\}=\{\lambda\}\cup\Sigma^+.$$

例 1 用归纳方法定义仅由整数，一目运算符 +，－，二目运算符 +，－，*，/ 及括号组成的算术表达式集合。

1° （基础语句）令 $D=\{0, 1, 2, \cdots, 9\}$，若 $x\in D^+$，则 x 是算术表达式。

2° （归纳语句） 如果 x 和 y 是算术表达式，则 $(-x)$，$(+x)$，$(x+y)$，$(x-y)$，$(x*y)$，(x/y) 是算术表达式。

3° （终结语句） 一个符号行是算术表达式，当且仅当它是有限次使用 1°，2° 得到的。

不难验证 341，0000，(3+7)，(3*(-61))，(+1-(+6/7)) 都是上面定义的集合中的元素。

习　　题

1. 下面的集合 A 和集合 B 是否是相等的？

(1) $A=\{1, 2, 3\}$，$B=\{x|x\in Z\}$。

(2) $A=\{1, 2, 4\}$，$B=\{1,2,2,4\}$。

(3) $A=\{a, b, ab\}$，$B=\{b,ab,a,b,a\}$。

2. 已知 $A\subseteq B$，$B\subset C$，证明 $A\subset C$。

3. 下面的等式是否成立？

(1) $\{0\}=\varnothing$，

(2) $\varnothing=0$，

(3) $\{\varnothing\}=\varnothing$,

(4) $\varnothing=\{x \mid x \neq x\}$,

(5) $\varnothing=\{B \mid B \subseteq A$ 且 $|B|=0\}$,

(6) $\mathscr{P}(\varnothing)=\varnothing$.

4. 下面的命题是否成立?

(1) 如果 $A \notin B, B \notin C$, 则 $A \notin C$.

(2) 如果 $a \notin A$, $A \supseteq B$, 则 $a \notin B$.

(3) $|\mathscr{P}(A)|>1$ 蕴涵 $A \neq \varnothing$.

5. 证明下列等式;

(1) $A \cap(\bar{A} \cup B)=A \cap B$.

(2) $A \cup(A \cap B)=A$.

(3) $A_1, A_2, \cdots, A_n$ 为集合,证明

$$\overline{\bigcap_i A_i}=\bigcup_i \overline{A_i} \quad ,$$

$$\overline{\bigcup_i A_i}=\bigcap_i \overline{A_i} \quad .$$

6. 证明下列命题:

(1) $B \subseteq C \Rightarrow (A \cap B) \subseteq (A \cap C)$.

(2) $A \subseteq C, B \subseteq C \Rightarrow (A \cup B) \subseteq C$.

(3) A 和 B 是有限集合,那么 $|A \cup B| \leqslant |A|+|B|$ 并且仅当 $A \cap B=\varnothing$ 时等式成立。

7. 用归纳法定义如下集合:

(1) 十进制无符号整数,它应该包括 4, 167, 0012 等,

(2) 带有限小数部分的无符号实数,它应该包括 6.1, 712., 61.200 等.

(3) 不以 0 打头的二进制偶整数,它应该包括 0, 110, 1010 等.

2 数论初步

数论是一个古老的数学分支。在本章中我们主要介绍初等数论中的基本知识，它包括整除性，同余式。原根与指数等内容，为第五章以后学习群、环，域的知识提供一个现实模型，也为今后学习保密通讯，密码体制作必要的准备。

2.1 整除性

在现实世界的数量关系中，人们首先认识到 1, 2, 3, … 这些正整数，在正整数之间可以做加法运算，为了能做减法运算又扩充到负整数和零。全体正整数构成了自然数集合 N。全体正负整数和零构成了整数集合 Z。整数集合和自然数集合是初等数论研究的对象。

在整数集合 Z 中可以进行加，减，乘运算，并且满足一些规律（例如，加法的交换律和结合律，乘法对加法的分配律等）。一般不能做除法运算，所以，研究整数间能否相除是揭示整数特性的一个重要手段。

2.1.1 整除关系及其性质

定义 2.1 a, b **为整数，**a **整除** b **当且仅当存在整数** d**，使得** $ad=b$**，并记为** $a|b$**，也称** a **是** b **的一个因子。**

整除性反映了两个整数之间的一种关系，如 $-3|6$，$3|-6$，$4\nmid 6$。

定理 2.1 **整除关系具有如下一些性质。设** $a, b, c, x, y\in Z$**。**

1° **对任何** a **均有** $a|a$**。**

2° **若 $a|b$ 且 $b|a$，则 $a=\pm b$。**

3° **若 $a|b$ 且 $b|c$，则 $a|c$。**

4° **若 $a|b$，则 $a|(bc)$。**

5° **若 $a|b$ 且 $a|c$，则 $a|(bx+cy)$。**

6° **若 $a,b>0$ 且 $a|b$，则 $a\leqslant b$。**

证明 1°，3°，4°，5°利用整除定义可以证明。这里只证明 2°和6°。

证明 2° 由 $a|b$ 和 $b|a$，知存在 $x,y\in \mathrm{Z}$，使得 $ax=b$，$by=a$。将它们的左边，右边相乘得到 $abxy=ab$，推出 $xy=1$。从而只能有两种情况 $x=y=1$ 或 $x=y=-1$，即 $a=b$ 或 $a=-b$。

证明 6° $a,b>0$ 且 $a|b$，必有 $x\in \mathrm{N}$ 使 $ax=b$。这里 $x\geqslant 1$，得出 $a\leqslant b$。更一般地，若 $a,b\in \mathrm{Z}$，且 $a,b\neq 0$，$a|b$，那么 $|a|\,|\,|b|$。由 6° 推出 $|a|\leqslant |b|$，即 $-|b|\leqslant a\leqslant |b|$。这表明非零的整数 b 只有有限多个因子。由于任何 $x\in \mathrm{Z}$，$x\cdot 0=0$，从而 0 有无限多个因子。**证毕**

2.1.2 最大公因子

有了整除的概念就可以定义两个整数的最大公因子。

定义 2.2 a,b **是两个不同时为零的整数，**a,b **的最大公因子** $d=(a,b)$ **满足**

1° $d|a$，$d|b$，**即** d **是** a **与** b **的公共因子。**

2° **若** $c|a$，$c|b$，**则** $c\leqslant d$，**即** d **是** a **与** b **的所有公共因子中最大的一个**

类似地可以定义$(a_1,a_2,\cdots,a_n)$。

一个整数至少有两个因子：1 和自身。两个整数至少有一个公因子 1。前面已经分析过，每个非零整数只有有限多个因子。从而当 a,b 不全为零时，它们的公因子也只有有限多个。d 则是最大的那个公因子。显然 $d=(a,b)\geqslant 1$。例如，$(-3,-6)=3$，$(-3,6)=3$，$(2,3)=1$。如果两个整数的最大公因子为 1，则称这两个整

数是互素的。

为了考察是否存在整数 x, y, 使得 a 与 b 的最大公因子 $d=ax+by$。也就是 a,b 的最大公因子 d 是否能用 a 与 b 线性表示出来。为此,我们先扩大范围研究集合

$$S=\{ax+by|x,\ y\in Z\}.$$

该集合有如下性质:

1° 若 $m,n\in S$,则 $m\pm n\in S$。

2° 若 $n\in S,c\in Z$,则 $cn\in S$。

3° 记 S 中最小正整数为 d, 那么 S 中每个数都是 d 的倍数。反过来,d 的每个倍数也必属于 S。

上面的性质 1°和 2°是显然的。现证明性质 3°。因为 a,b 不全为零,$\pm a$, $\pm b$ 显然属于集合 S。也就是说,集合 S 中有正元素,所以 S 中一定存在着一个最小的正整数 d。任取 $c\in S$, 有 $c=qd+r$,其中 q 和 r 分别为 c 除以 d 得到的商和非负余数,$0\leqslant r<d$。因为 $d\in S$,由性质 2° 知 $q\cdot d\in S$。又因 $c\in S$,由性质 1° 知 $r=c-q\cdot d\in S$。由于 d 是 S 中最小的正整数,从而必有 $r=0$, 即 $c=q\cdot d$,故

$$S=\{ax+by|x,y\in Z\}=\{k\cdot d|k\in Z\}.$$

下面证明 S 的最小正整数 d 就是 a 与 b 的最大公因子.由于 $d\in S$, 存在 x_0, $y_0\in Z$,使得 $d=ax_0+by_0$。因为 $(a,\ b)|a,(a,b)|b$, 于是 $(a,\ b)|d$。由整除的性质 6°, 知 $(a,\ b)\leqslant d$。另一方面, 因为 $a\in S$, $b\in S$, 那么存在 k_1, $k_2\in Z$, 使得 $a=k_1d$, $b=k_2d$,从而 d 是 a 与 b 的公因子。而$(a,\ b)$是 a 与 b 的最大公因子, 所以 $d\leqslant(a,b)$。综上知 $d=(a,b)$。

从上面的讨论看出,若 a,b 是不全为零的整数,那么一定存在整数 x,y 使 $ax+by=(a,b)$。另外,整数 n 可以表示成 $ax+by$ 形式的充要条件是$(a,\ b)|n$。显然,当 a 与 b 互素时,任何整数 n 都可以表示成 $ax+by$ 的形式,由此得到

定理 2.2 设 a, b 是不全为零的整数, 那么

1° (a, b)**是集合** $S=\{ax+by \mid x,y\in Z\}$**中最小的正整数。**

2° **整数** n **可以表示成** $ax+by$ **形式的充要条件是**$(a,b)\mid n$。

利用定理 2.2 可以得到关于最大公因子的一些有用的性质：

推论 2.1 若 m **为正整数，则**$(ma, mb)=m(a, b)$。

证明 $(ma,mb)=$形如 $max+mby$ 的最小正整数

$=m\cdot$形如 $ax+by$ 的最小正整数

$=m\cdot(a, b)$。

特别有

1° 若$(a, b)=d$，则 $d=(a, b)=d\left(\frac{a}{d}, \frac{b}{d}\right)$。两边除以 d，得到$\left(\frac{a}{d}, \frac{b}{d}\right)=1$。

2° 若 m 是 a 与 b 的公因子，$a=ma_1$，$b=mb_1$。$(a,b)=m(a_1,b_1)$，所以 $m\mid(a, b)$，即 a 与 b 的公因子是最大公因子的因子。**证毕。**

推论 2.2 若$(a, m)=(b, m)=1$，**则**$(ab, m)=1$。

证明 由$(a,m)=(b,m)=1$ 知存在 $x_0, y_0, x_1, y_1\in Z$，使得 $ax_0+my_0=1$，$bx_1+my_1=1$。将这两个式子左右两边相乘，得到

$$abx_0x_1+m(ax_0y_2+bx_1y_0+my_0y_1)=1.$$

从而$(ab, m)=1$。**证毕**

推论 2.3 a，b **是不全为零的整数，对任意整数** x **有**$(a, b)=(a,b+ax)$。

证明 令 $g=(a, b)$，$h=(a, b+ax)$。由 $g\mid a, g\mid b$，知$g\mid(b+ax)$，即 g 是 a 与 $b+ax$ 的公因子。从推论 2.1 中的 2°知 $g\mid h$。另一方面 $h\mid a, h\mid(b+ax)$，推出 $h\mid b$。从而 h 是 a 与 b 的公因子。同理 $h\mid g$。由定理 2.1 中 2° 和 $h, g>0$，得出 $h=g$，即$(a, b)=(a,b+ax)$。**证毕**

推论 2.4 若 $c\mid ab$ 且$(c, b)=1$，则 $c\mid a$。

证明 由 $c|ab, c|ac$，根据推论 2.1 中的 2° 知 $c|(ab, ac)$。而从推论 2.1 知 $(ab, ac)=a(b, c)=a\cdot 1=a$。于是 $c|a$。**证毕**

上面在证明 (a, b) 可表示成 $ax+by$ 形式的过程中，没有给出一种可行的方法求出 x 和 y。我们利用推论 2.3，可以得到求解 $ax+by=(a, b)$ 的欧几里得算法。由于 $(a, b)=(|a|, |b|)$，我们这里不妨假设 $a\geqslant b>0$。

定理 2.3 a, b **为正整数，有下列关系式**

$$
\begin{aligned}
a&=bq_0+r_0, & 0<r_0<b,\\
b&=r_0q_1+r_1, & 0<r_1<r_0,\\
r_0&=r_1q_2+r_2, & 0<r_2<r_1,\\
&\cdots\cdots\\
r_i&=r_{i+1}q_{i+2}+r_{i+2}, & 0<r_{i+2}<r_{i+1},\\
r_{i+1}&=r_{i+2}q_{i+3},
\end{aligned}
$$

则 $(a, b)=r_{i+2}$。

证明 在上述辗转相除的一系列关系式中，$b>r_0>r_1>\cdots>r_{i+1}>r_{i+2}>\cdots\geqslant 0$ 是一个非负的递减序列。因此经过数次相除以后所得的余数必为 0。我们这里假设 $r_{i+3}=0$。根据推论 2.3 有

$$
\begin{aligned}
(a, b)&=(b, r_0)=(r_0, r_1)=\cdots=(r_i, r_{i+1})=(r_{i+1}, r_{i+2})\\
&=r_{i+2}。
\end{aligned}
$$

证毕

由上述辗转相除算法，不仅可以得到 (a, b)，利用这些关系式反推回去，就可以得到 $(a, b)=ax+by$ 中的 x, y 的值。

例 1 计算 $(936, 657)$。

解 按定理 2.3 提供的辗转相除算法得到关系式

$$
\begin{aligned}
936&=657\cdot 1+306,\\
657&=306\cdot 2+45,\\
306&=45\cdot 6+36,\\
45&=36\cdot 1+9,\\
36&=9\cdot 4,
\end{aligned}
$$

于是 $(936, 657)=9$。

又有

$$9=45-36\cdot1=45-(306-45\cdot6)=45\cdot7-306$$
$$=(657-306\cdot2)\cdot7-306=657\cdot7-306\cdot15$$
$$=657.7-(936-657\cdot1)\cdot=657\cdot22-936\cdot15,$$

方程 $936x+657y=9$ 的解为 $x=-15, y=22$。

2.1.3 最小公倍数

定义 2.3 a, b **为整数，** a **与** b **的最小公倍数** $c=[a, b]$**满足**

1° $a|c, b|c$ 且 $c>0$。

2° 若 $a|e, b|e$，则 $c\leqslant|e|$。

类似地可以定义$[a_1, a_2, \cdots, a_n]$。

任何两个整数 a,b 存在着正公倍数，如$|ab|$。我们知道，若 u 是 a 与 b 的公倍数，则对于任何正整数 x，ux 也是 a 与 b 的公倍数。所以 a 与 b 不存在最大公倍数。显然 a 与 b 有最小正公倍数 c。我们称 c 为 a 与 b 的最小公倍数。

对于两个非零整数的最小公倍数也有类似于最大公因子的结论。

定理 2.4 a,b **为非零整数，**a **与** b **的每个公倍数均是最小公倍数的倍数.**

证明 考虑集合 $S'=\{a$ 与 b 的所有公倍数$\}$。该集合有如下性质。

1° 若 $m, n\in S'$，则 $m\pm n\in S'$。

2° 若 $n\in S'$，$c\in Z$，则 $cn\in S'$。

3° S' 中有最小正整数 u，那么 S' 中每个元素均是 u 的倍数。反过来 u 的任意倍数必属于 S'。显然 u 就是 a 与 b 的最小公倍数。

1°，2°是显然的。因 S' 是由 a 与 b 的所有公倍数组成的，$\pm ab\in S'$，即 S' 中有正数，从而 S' 中有最小正整数 u。任取 $v\in S'$，$v=qu+r$，$0\leqslant r<u$。由于 v，$u\in S'$，$q\in Z$，所以 $r=v$

$-qu \in S'$。u 是 S' 中的最小正整数，因此必有 $r=0$，即 $v=qu$。由 a 与 b 的最小公倍数的定义知 $u=[a,b]$。$S'=\{ku|k\in Z\}$。这说明非零整数 a,b 的每个公倍数都是最小公倍数的倍数。**证毕**

利用定理 2.4 可以得到关于最小公倍数的一些有用的性质。

推论 2.5 m 为正整数，$[ma,mb]=m[a,b]$。

证明 由 $a|[a,b]$，$b|[a,b]$，知 $ma|m[a,b]$，$mb|m[a,b]$，即 $m[a,b]$ 是 ma 与 mb 的公倍数，从而 $[ma,mb]|m[a,b]$。另一方面，若 l 是 ma 与 mb 的公倍数，必有 $m|l$。不妨令 $l=l'm$，那么 l' 是 a 与 b 的公倍数，从而 $[a,b]|l'$。由此推出 $m[a,b]|l$，现取 $l=[ma,mb]$，得到 $m[a,b]|[ma,mb]$。由定理 2.1 中 2° 以及 $m[a,b]>0$，$[ma,mb]>0$。最后得出

$$[ma,mb]=m[a,b].$$

证毕

论推 2.6 $[a,b](a,b)=ab$。

证明 首先讨论 $(a,b)=1$ 的情况。$[a,b]$ 是 a 与 b 的最小公倍数，存在 m_1 使得 $[a,b]=m_1a$。由 $b|[a,b]$，知 $b|m_1a$。而 $(a,b)=1$，由推论 2.4 得出 $b|m_1$。m_1 应该是满足此关系的最小正整数，所以 $m_1=b$，即 $[a,b]=ab$。

当 $(a,b)=d$ 时，由推论 2.1 中的 1° 知 $\left(\frac{a}{d},\frac{b}{d}\right)=1$。从上面的结论，有 $\left[\frac{a}{d},\frac{b}{d}\right]=\frac{1}{d^2}ab$。根据推论 2.1 和推论 2.5

$$(a,b)[a,b]=d^2\left(\frac{a}{d},\frac{b}{d}\right)\left[\frac{a}{d},\frac{b}{d}\right]=d^2\cdot 1\cdot\frac{1}{d^2}\cdot ab=ab.$$

这正是所要的结论。**证毕**

2.1.4 素因子分解唯一性定理

a 是 b 的因子当且仅当 $a|b$。如果正整数 b 只有 1 和 b 为其因子，则称 b 为素数。例如 2，3，5，7，11，13，17，19，…，每个大于 1 的整数都可以被一个素数整除，从而得到该整数的素因子分

解式。例如 $60=2^2\cdot 3\cdot 5$。如果不考虑因子出现的次序，那么这种分解形式是唯一的。我们只叙述素因子分解唯一性定理，而不加以证明。

定理 2.5 （素因子分解唯一性定理）

任意正整数都能用一种方式且只有一种方式写成素数的乘积。

我们可以用加法作为构造自然数的手段，任何正整数 $n=\overbrace{1+1+\cdots+1}^{n}$，其基本元素就是1。当用乘法作为构造自然数的手段时，其基本元素是全体素数。这个结论是素因子分解唯一性定理告诉我们的。

那么有多少个素数呢?结论是：存在着无限多个素数。可用反证法证明这一结论。假若只有有限多个素数 $p_1, p_2, \cdots, p_k$。令 $n=p_1p_2\cdots p_k+1$。n 是自然数，存在一个素数 p_i 使 $p_i|n$，推出 $p_i|1$。产生矛盾，故不可。所以有无限多个素数。

一般来说，对给定的整数进行素因子分解是很困难的。首先遇到的问题是没有一种“可行性算法”来确定所给的整数是否是素数。奥地利天文学家用厄氏筛法花了20年时间得到了 10^8 以内的素数。60年代美国宣布他们在计算机内存放着前 5×10^8 个素数.85年9月美国在CRAY X-MP超级计算机上计算的最大素数为 $2^{216091}-1>10^{65050}$。这是目前人们知道的最大素数。

2.2 线性不定方程

限制在某类数中(如，正整数，有理数等)求解的方程叫丢番图方程。最简单的丢番图方程就是线性不定方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n=n$$

求其整数解。

早在1400多年前，隋朝“张丘健算径”一书中最后一问是世界

著名的百鸡问题。问题是：鸡翁一，值钱五，鸡母一，值钱三，鸡仔三，值钱一，百钱买百鸡，问鸡翁、鸡母、鸡仔各几何？设鸡翁 x 只，鸡母 y 只，鸡仔 $3z$ 只。由题意列出方程

$$\begin{cases} 5x+3y+z=100 \\ x+y+3z=100. \end{cases}$$

消去 z，得到 $7x+4y=100$。这时多元线性不定方程化为二元线性不定方程。

以下我们只讨论二元线性不定方程。

定理 2.6 a,b,n **为整数**. $ax+by=n$ **有解当且仅当** $(a,b)|n$. **如果** x_0,y_0 **是** $ax+by=n$ **的一组解，则通解为**

$$x=x_0+\frac{b}{(a,b)}t,\qquad y=y_0-\frac{a}{(a,b)}t,$$

其中 t **为整数。**

证明 由上节定理 2.2 对集合 $S=\{ax+by|x,y\in\mathbf{Z}\}$ 的讨论知 $ax+by=n$ 有解当且仅当 $(a,b)|n$.

如果 x_0,y_0 是 $ax+by=n$ 的一组解，即 $ax_0+by_0=n$. 由于

$$a\left(x_0+\frac{b}{(a,b)}t\right)+b\left(y_0-\frac{a}{(a,b)}t\right)=n,$$

所以 $x=x_0+\frac{b}{(a,b)}t$，$y=y_0-\frac{a}{(a,b)}t$ 是 $ax+by=n$ 的解。反过来，若 x,y 是方程 $ax+by=n$ 的解，则

$$a(x-x_0)+b(y-y_0)=0.$$

由此得出 $b|a(x-x_0)$，即 $\frac{b}{(a,b)}\Big|\frac{a}{(a,b)}(x-x_0)$. 而 $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$，于是 $\frac{b}{(a,b)}\Big|(x-x_0)$，即 $x=x_0+\frac{b}{(a,b)}t$，其中 t 为一个整数。将 x 的表达式代入 $a(x-x_0)+b(y-y_0)=0$，解出 $y=y_0-\frac{a}{(a,b)}t$. 由此可知该方程的通解为

$$x=x_0+\frac{b}{(a,b)}t,\qquad y=y_0-\frac{a}{(a,b)}t.$$

证毕。

例1 前面的百鸡问题 $7x+4y=100$。因 $(7,4)=1$，所以方程有解，$x_0=0$，$y_0=25$ 是一组特解。通解为 $x=4t$，$y=25-7t$。为了保证 x,y 为正整数，t 只能取值 0，1，2，3。故该方程的解共有四组。它们是

$$\begin{cases}x=0\\ y=25\\ 3z=75,\end{cases}\quad \begin{cases}x=4\\ y=18\\ 3z=78,\end{cases}\quad \begin{cases}x=8\\ y=11\\ 3z=81,\end{cases}\quad \begin{cases}x=12\\ y=4\\ 3z=84.\end{cases}$$

2.3 同余式与线性同余方程

2.3.1 同余式及其性质

在第一节中我们讲到整除性。整数 a 除以整数 b，如果余数为 0，称作 $b|a$。当 $b\nmid a$ 时，余数有各种可能性。为了区分它们，我们引入同余的概念。

定义 2.4 设 $a, b, m\in \mathbb{Z}$，$m\neq 0$，a 与 b 模 m 同余当且仅当 $m|(a-b)$，并记为 $a\equiv b(\bmod m)$。

显然 $a\equiv b(\bmod m)$ 与 $a\equiv b(\bmod -m)$ 等价。所以，以后假设 $m>0$。

同余式有许多与通常等式相类似的性质。我们列举如下：(设 $a, b, c, x, y\in \mathbb{Z}$)。

1° $a\equiv a(\bmod m)$。

2° 若 $a\equiv b(\bmod m)$，则 $b\equiv a(\bmod m)$。

3° 若 $a\equiv b(\bmod m)$，$b\equiv c(\bmod m)$，则 $a\equiv c(\bmod m)$。

4° 若 $a\equiv b(\bmod m)$，$c\equiv d(\bmod m)$，则

$$a+c\equiv b+d(\bmod m),\quad ac\equiv bd(\bmod m).$$

5° 若 $a\equiv b(\bmod m)$ 且 $d|m$，则 $a\equiv b(\bmod d)$。

6° 若 $a\equiv b(\bmod m)$，则 $ax\equiv bx(\bmod m)$。

7° $ax \equiv ay \pmod{am}$ 当且仅当 $x \equiv y \pmod{m}$

8° 若 $ax \equiv ay \pmod{m}$ 且 $(a, m) = 1$，则 $x \equiv y \pmod{m}$。

9° $x \equiv y \pmod{m_i}$，$1 \leqslant i \leqslant r$ 当且仅当 $x \equiv y (\mathrm{mod}\ [m_1, m_2, \cdots, m_r])$。

以上诸性质都可以用同余定义直接得到。证明从略。

2.3.2 线性同余方程

a, b 为整数，我们要求线性同余方程 $ax \equiv b \pmod{m}$ 的解。先看一个特殊情况。

定理 2.7 **设 $(a, m) = 1$。对于每个整数 b，同余方程 $ax \equiv b \pmod{m}$ 有模 m 唯一解。**

证明 因为 $(a, m) = 1$，对每个整数 b 都存在着 $x, y \in Z$，使得 $ax + my = b$，即 $ax \equiv b \pmod{m}$。x 就是该同余方程的解。

下面证明解是模 m 唯一的。若 x_1, x_2 都是 $ax \equiv b \pmod{m}$ 的解，即 $ax_1 \equiv ax_2 \equiv b \pmod{m}$。由于 $(a, m) = 1$，得到 $x_1 \equiv x_2 \pmod{m}$。这说明方程的任意两个解是模 m 同余的，即解模 m 唯一。证毕。

定理 2.8 **同余方程 $ax \equiv b \pmod{m}$ 有解当且仅当 $(a, m) \mid b$。当条件满足时，该同余方程有 (a, m) 个模 m 不同余的解**

$$x = x_0 + \frac{m}{(a, m)} t \pmod{m}, \quad 0 \leqslant t \leqslant (a, m) - 1.$$

其中 x_0 是同余方程

$$\frac{a}{(a, m)} x \equiv \frac{b}{(a, m)} \left(\mathrm{mod}\ \frac{m}{(a, m)} \right)$$

的解。

证明 设 x_0 是同余方程 $ax \equiv b \pmod{m}$ 的解。即 $m \mid (ax_0 - b)$。由于 $(a, m) \mid m$，显然有 $(a, m) \mid (ax_0 - b)$。又由 $(a, m) \mid a$，推出 $(a, m) \mid b$。反过来，当 $(a, m) \mid b$ 时，存在 $x_1, y_1 \in Z$，使 $ax_1 + my_1 = b$，即 $ax_1 \equiv b \pmod{m}$。这表明 x_1 就是同余方程 $ax \equiv b \pmod{m}$

的一个解。

当满足同余方程有解的条件$(a,m)|b$时，$ax\equiv b \pmod m$可以化成等价的同余方程

$$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}\quad\left(\bmod \frac{m}{(a,m)}\right).$$

由于$\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right)=1$，该方程有模$\frac{m}{(a,m)}$唯一解$x\equiv x_0$ $\left(\bmod \frac{m}{(a,m)}\right)$。这里不妨取$0\leqslant x_0<\frac{m}{(a,m)}$.这个$x_0$也是$ax\equiv b$ $(\bmod m)$的一个解。下面证明$x_0+i\frac{m}{(a,m)}$，$0\leqslant i\leqslant (a,m)-1$，也是$ax\equiv b \pmod m$的解。把它们代入方程

$$a\left(x_0+i\frac{m}{(a,m)}\right)=ax_0+\frac{a}{(a,m)}im\equiv b\quad(\bmod m).$$

而

$$0\leqslant x_0+i\frac{m}{(a,m)}<\frac{m}{(a,m)}+((a,m)-1)\frac{m}{(a,m)}=m,$$

所以$x_0+i\frac{m}{(a,m)}$，$0\leqslant i\leqslant (a,m)-1$是$(a,m)$个模$m$不同余的解。反过来，假设$y$是$ax\equiv b \pmod m$的一个解。必有$ax_0\equiv ay\equiv b$ $(\bmod m)$，推出$x_0\equiv y\left(\bmod \frac{m}{(a,m)}\right)$，即$y=x_0+k\frac{m}{(a,m)}$。令$i$表示$k$除以$(a,m)$的非负余数，那么$y\equiv x_0+i\frac{m}{(a,m)} \pmod m$。这说明$ax\equiv b \pmod m$除上述$(a,m)$个解之外没有其它形式的解。**证毕。**

例1 解$14x\equiv 27 \pmod{31}$。

解 因$(14,31)=1$，$14x\equiv 27 \pmod{31}$。有模31唯一解。

$$14x\equiv 27\equiv 58\quad(\bmod 31).$$

因$(2,31)=1$，利用同余式性质8°得到

$$7x\equiv 29\quad(\bmod 31).$$

又由
$$7x\equiv 29\equiv 91\quad(\bmod 31),$$

且(7，31)=1，解出 $x\equiv 13 \pmod{31}$。

例 2 解 $6x\equiv 30 \pmod{33}$。

解 $(6,33)=3$ 且 $3|30$，由定理 2.8 知该同余方程有 3 个模 33 不同余的解。

与 $6x\equiv 30 \pmod{33}$ 等价的同余方程 $2x\equiv 10 \pmod{11}$ 中 $(2,11)=1$，$x\equiv 5 \pmod{11}$ 是它的模 11 唯一解。$x\equiv 5+11t \pmod{33}$，$0\leqslant t\leqslant 2$ 是同余方程 $6x\equiv 30 \pmod{33}$ 的三个模 33 不同余的解，即该同余方程的解为

$$x\equiv 5,16,27 \pmod{33}.$$

2.3.3 求解线性同余方程组

我国古代数学著作“孙子算经”中有“物不知其数”一问：“今有物不知其数。三三数之余二，五五数之余三，七七数之余二，问物几何?”用数学语言来描述就是(设其数为 x)

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 2 \pmod 7. \end{cases}$$

这一问题的古代算法在程大位的“算法统宗”中总结成

“三人同行七十稀，
五树梅花廿一枝，
七子团圆月正半，
除百零五便得知。”

意思是以 70，21，15 分别乘该数除以 3，5，7所得的余数 2，3，2，将结果相加再模 105。即

$$x\equiv 70\cdot 2+21\cdot 3+15\cdot 2=233\equiv 23 \pmod{105}.$$

国外数论文献中把这个算法称之为中国剩余定理。在下面定理中将给出证明。

定理 2.9 设自然数 $m_1, m_2, \cdots, m_r$ 两两互素。对任意整数 $a_1, a_2, \cdots, a_r$ 线性同余方程组 $x\equiv a_i \pmod{m_i}$，$1\leqslant i\leqslant r$，均有解，

并且解是模 $m_1m_2\cdots m_r$ 唯一的。

证明 令 $M=m_1m_2\cdots m_r$，$M_i=\frac{M}{m_i}$，$(M_i,\ m_i)=1$，$1\leqslant i\leqslant r$。对每个 i，$M_ib_i\equiv1(\bmod m_i)$有解并且当 $j\neq i$ 时，$M_jb_i\equiv0(\bmod m_i)$。现令 $y=\sum_{j=1}^{r}M_jb_ja_j$，显然

$$y\equiv M_ib_ia_i\equiv a_i(\bmod m_i),\ 1\leqslant i\leqslant r,$$

从而 y 是同余方程组的解。同时与 y 模 $m_1m_2\cdots m_r$ 同余的数也是该同余方程组的解。

令 y_1，y_2 都是同余方程组的解，那么 $y_1-y_2\equiv0(\bmod m_i)$，$1\leqslant i\leqslant r$。也就是说 y_1-y_2 是 m_1，m_2，…，m_r 的公倍数，从而 $[m_1,\ m_2,\ \cdots,\ m_r]\mid(y_1-y_2)$；而 m_1，m_2，…，m_r 两两互素，$[m_1,\ m_2,\ \cdots,\ m_r]=m_1m_2\cdots m_r$，最后得出

$$y_1\equiv y_2\quad(\bmod m_1m_2\cdots m_r).$$

证毕。

该定理的证明是构造性的，它已指明解线性同余方程组的具体步骤。

例 1 解同余方程组

$$\begin{cases}x\equiv2 & (\bmod 3)\\ x\equiv3 & (\bmod 5)\\ x\equiv2 & (\bmod 7).\end{cases}$$

解 本题中 $M=3\cdot5\cdot7=105$，$M_1=35$，$M_2=21$，$M_3=15$。由 $35b_1\equiv1(\bmod 3)$，$21b_2\equiv1(\bmod 5)$，$15b_2\equiv1(\bmod 7)$ 分别解出 $b_1=2$，$b_2=1$，$b_3=1$。从而

$$\begin{aligned}y&=35\cdot2\cdot2+21\cdot1\cdot3+15\cdot1\cdot2\\&=70\cdot2+21\cdot3+15\cdot2=233.\end{aligned}$$

$y\equiv23(\bmod 105)$是该同余方程组的解。

定理 2.10 线性同余方程组 $x\equiv a_i(\bmod m_i)$，$i=1,2$，有解的充要条件是$(m_1,\ m_2)\mid(a_1-a_2)$。在条件满足时，该方程组的解

模 $[m_1, m_2]$ 唯一.

证明 该方程组有解就是存在着整数 s, t, 使 $x = m_1t + a_1$ 且 $x = m_2s + a_2$, 即 $m_1t - m_2s = a_2 - a_1$. 从定理 2.6 知该方程有解当且仅当 $(m_1, m_2) | (a_2 - a_1)$. 所以线性同余方程组有解的充要条件是 $(m_1, m_2) | (a_1 - a_2)$.

若当条件满足时, x_1 和 x_2 都是该方程组的解, 则

$$\begin{cases} x_1 - x_2 \equiv 0 \pmod{m_1} \\ x_1 - x_2 \equiv 0 \pmod{m_2}. \end{cases}$$

$x_1 - x_2$ 是 m_1, m_2 的公倍数. 于是 $[m_1, m_2] | (x_1 - x_2)$, 即 $x_1 \equiv x_2 \pmod{[m_1, m_2]}$. 它说明该方程组的解模 $[m_1, m_2]$ 唯一. **证毕.**

例 2 求解

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 0 \pmod 6. \end{cases}$$

解 因 $(4, 6) | (2 - 0)$, 该方程组有解并且解模 12 唯一. 下面就求它的解. 由 $x \equiv 2 \pmod 4$, 知 $x = 2 + 4k_1$. 将 x 代入 $x \equiv 0 \pmod 6$. 得到 $4k_1 \equiv 4 \pmod 6$, 化简后为 $k_1 \equiv 1 \pmod 3$. 于是 $k_1 = 1 + 3k_2$. 再代入 $x = 2 + 4k_1$, 得到 $x = 6 + 12k_2$. 从而解为

$$x \equiv 6 \pmod{12}.$$

2.4 欧拉定理及欧拉函数

2.4.1 完系与缩系

对于给定的整数 m, 每个整数都与且仅与集合 $\{0, 1, \cdots, m-1\}$ 中一个数模 m 同余. 一般地,

定义 2.5 整数集合 $\{x_1, x_2, \cdots, x_m\}$, 如果每个整数都与且仅与该集合中一个 x_i 模 m 同余, 则称 $\{x_1, x_2, \cdots, x_m\}$ 为模 m 的完系.

显然 $\{0, 1, 2, 3, 4\}$ 是模 5 的完系, $\{10, 21, 27, 38, -1\}$ 也是

模 5 的完系。不难看出，模 m 的完系有两个特征，首先它是由 m 个元素组成的，其次这些元素相互不模 m 同余。

我们把模 m 的同余类表示成 $A_i=\{x|x\in Z, x\equiv i(\bmod m)\}$，$0\leqslant i\leqslant m-1$。每个整数都与 $\{0, 1, \cdots, m-1\}$ 中一个数同余，所以每个整数只属于 $A_0, A_1, \cdots, A_{m-1}$ 中的一个。若 $x\in A_i$ 且 $(x, m)=1$，那么 A_i 中的任意元素 y 都必有 $(y, m)=1$。这是因为 $x, y\in A_i, x\equiv y(\bmod m)$，即 $x=y+km$。如果 $(y,m)=d$，则必有 $d|x$。再由 $d|m$ 知 $d|(x,m)$。而 $(x, m)=1$，从而 $(y,m)=d=1$。

若 $x\in A_i$ 且 $(x,m)=1$，则称 A_i 是与 m 互素的同余类。与 m 互素的同余类个数记为 $\phi(m)$，称为欧拉函数。

定义 2.6 **在每个与 m 互素的同余类中取一个元素作为代表放在一起构成的集合 $\{r_1, r_2, \cdots, r_{\phi(m)}\}$ 叫做模 m 的缩系。**

例 1 $\{0,1,2,3,4,5\}$ 是模 6 的完系，六个同余类 $A_i=\{6k+i|k\in Z\}, 0\leqslant i\leqslant 5$ 中 A_1, A_5 是与 6 互素的同余类，故 $\phi(6)=2$。$\{1,5\}$，$\{7,-1\}$ 都是模 6 的缩系。

实际上，把 $\{1, 2, \cdots, m-1\}$ 中与 m 互素的数放在一起就恰好是模 m 的一个缩系。$\phi(m)$ 就是不超过 m 且与 m 互素的正整数个数。不难验证，$\phi(2)=1, \phi(3)=\phi(4)=\phi(6)=2, \phi(5)=\phi(8)=4$，$\phi(7)=6$。我们规定 $\phi(1)=1$。显然对于素数 p，$\phi(p)=p-1$。

引理 2.1 已知 $(a, m)=1$。若 $\{x_1, x_2, \cdots, x_m\}$ 是模 m 的完系，则 $\{ax_1, ax_2, \cdots, ax_m\}$ 也是模 m 的完系，若 $\{r_1, r_2, \cdots, r_{\phi(m)}\}$ 是模 m 的缩系，则 $\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$ 也是模 m 的缩系。

证明 $\{x_1, x_2, \cdots, x_m\}$ 是模 m 的完系，由其定义知 $i\neq j$，$x_i\not\equiv x_j(\bmod m)$。如果 $ax_i\equiv ax_j(\bmod m)$，由于 $(a, m)=1$，推出必有 $x_i\equiv x_j(\bmod m)$。这与 $\{x_1, x_2, \cdots, x_m\}$ 是模 m 的完系矛盾。由此得出 $ax_1, ax_2, \cdots, ax_m$ 是两两模 m 互不同余的 m 个元素，它们正好构成一个模 m 的完系。

$\{r_1, r_2, \cdots, r_{\phi(m)}\}$ 是模 m 的缩系，由其定义知 $(r_i, m)=1$，

$1 \leqslant i \leqslant \phi(m)$，并且 $i \neq j$ $r_i \not\equiv r_j \pmod m$。从$(r_i, m)=1$ 和$(a, m)=1$，根据推论 2.2 知$(ar_i, m)=1$。前面已经证明过 $i \neq j$，$ar_i \not\equiv ar_j \pmod m$。$ar_1, ar_2, \cdots, ar_{\phi(m)}$ 恰是 $\phi(m)$个与 m 互素且两两模 m 不同余的元素。它们恰好构成模 m 的一个缩系。 **证毕。**

2.4.2 欧拉定理与费尔马定理

定理 2.11 （欧拉定理）

如果$(a,m)=1$，**则** $a^{\phi(m)} \equiv 1 \pmod m$。

证明 取一个模 m 的缩系$\{r_1, r_2, \cdots, r_{\phi(m)}\}$。当$(a, m)=1$时、$\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$也是模 m 的缩系。任选一个 r_i，必存在一个 r_j 使 $r_i \equiv ar_j \pmod m$，并且不同的下标 i 对应不同的下标 j。由此得出

$$r_1 r_2 \cdots r_{\phi(m)} \equiv ar_{j_1} \cdot ar_{j_2} \cdots ar_{j_{\phi(m)}}$$
$$= a^{\phi(m)} \cdot r_1 r_2 \cdots r_{\phi(m)} \pmod m.$$

由于$(r_i, m)=1$，$1 \leqslant i \leqslant \phi(m)$，根据推论 2.2 知

$$(r_1 r_2 \cdots r_{\phi(m)}, m)=1,$$

从前式立即推出

$$a^{\phi(m)} \equiv 1 \pmod m.$$

证毕。

在定理 2.11 中取 m 为素数 p，$(a,p)=1$ 就是 $p \nmid a$，$\phi(p) = p-1$。从而得到费尔马定理：p 为素数且 $p \nmid a$，则

$$a^{p-1} \equiv 1 \pmod p.$$

若 $p|a$，$a \equiv 0 \pmod p$，则显然成立 $a^p \equiv a \pmod p$。而当 $p \nmid a$ 时，从费尔马定理知 $a^{p-1} \equiv 1 \pmod p$。再由同余式性质 6°，仍成立 $a^p \equiv a \pmod p$。所以，对于任何 a 都有 $a^p \equiv a \pmod p$，其中 p 是素数。

2.4.3 计算欧拉函数

引理 2.2 p **为素数，对一切正整数** n，$\phi(p^n) = p^{n-1}(p-1)$。

证明 小于等于 p^n 的数共有 p^n 个，其中与 p^n 有公因子 p 的数是 $p, 2p, \cdots, p^{n-1}p$，一共有 p^{n-1} 个。那么与 p^n 无公因子 p 的，即与 p^n 互素的数共有 $p^n - p^{n-1} = p^{n-1}(p-1)$ 个。**证毕。**

定理 2.12 当 $(m, n) = 1$ 时，$\phi(mn) = \phi(m)\cdot\phi(n)$。

证明 $\phi(mn)$ 是小于等于 mn 且与 mn 互素的正整数个数，下面把所有小于等于 mn 的正整数列成一个方阵

$$
\begin{array}{lllll}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & & & & \\
m & m+m & 2m+m & \cdots & (n-1)m+m.
\end{array}
$$

若 $(m, r) = d > 1$，那么 r 所在行的全部元素 $r, m+r, 2m+r, \cdots, (n-1)m+r$ 均与 mn 有公因子 d。由此可知，与 mn 互素的数只能在 $(m, r) = 1$ 的 $\phi(m)$ 行中寻找，而当 $(m, r) = 1$ 时，$\{r, m+r, 2m+r, \cdots, (n-1)m+r\}$ 是 n 元集合，并且两两模 n 不同余。它是模 n 的完系。在一个模 n 的完系中有 $\phi(n)$ 个数与 n 互素。而该完系中每个数均与 m 互素，从而它里面有 $\phi(n)$ 个数与 mn 互素。

从上分析得到 $\phi(mn) = \phi(m)\cdot\phi(n)$。**证毕。**

若 $(m, n) = 1$，满足 $f(mn) = f(m)f(n)$ 的函数称为积性函数。欧拉函数 ϕ 是积性函数。从定理 2.12 不难看出，若 n 的素因子分解式为 $n = p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$，则

$$\phi(n) = p_1^{l_1-1}(p_1 - 1)\cdots p_k^{l_k-1}(p_k - 1) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

例 1 求 2^{340} 除以 341 的余数。

解 $341 = 11\cdot 31$。由欧拉定理知 $2^{10} \equiv 1 \pmod{11}$ $2^{30} \equiv 1 \pmod{31}$。

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11},$$

$$2^{340} = (2^{30})^{11}\cdot 2^{10} \equiv 2^{10} = (2^5)^2 \equiv 1 \pmod{31},$$

即 2^{340} 是下面线性同余方程组的解。

$$\begin{cases} x\equiv 1 \pmod{11} \\ x\equiv 1 \pmod{31}. \end{cases}$$

解得 $x\equiv 1 \pmod{341}$，即 $2^{340}\equiv 1 \pmod{341}$。

本例说明费尔马定理的逆定理不成立，$2^{340}\equiv 1 \pmod{341}$，但是 $2|340$。

例 2 解 $9x\equiv 7 \pmod{13}$。

解 13 是素数。由费尔马定理知 $3^{12}\equiv 1 \pmod{13}$。

$$x\equiv 3^{12}\cdot x\equiv 3^{10}\cdot 9x\equiv 3^{10}\cdot 7\equiv (13-4)^5\cdot 7\equiv (-4)^5\cdot 7$$
$$\equiv (13+3)^2(-28)\equiv 9\cdot(-2)\equiv 8 \pmod{13},$$

$x\equiv 8 \pmod{13}$ 是该方程的解。

2.4.4 威尔逊定理

威尔逊定理给出了判定素数的充要条件。为此先给出两个引理。

引理 2.3 **$x^2\equiv 1 \pmod p$ 恰好有两个解 $x\equiv 1, p-1 \pmod p$。**

证明 $x^2\equiv 1 \pmod p$ 是二次同余方程。设 r 是其解，$r^2-1\equiv 0 \pmod p$，即 $p|(r+1)(r-1)$。这里有两种可能；若 $p|(r+1)$，则 $r\equiv p-1 \pmod p$；若 $p|(r-1)$，则 $r\equiv 1 \pmod p$。**证毕。**

引理 2.4 **p 为奇素数，a' 表示线性同余方程 $ax\equiv 1 \pmod p$ 的解。这里 a 可以取值 $1, 2, \cdots, p-1$。当 $a\not\equiv b \pmod p$ 时，$a'\not\equiv b' \pmod p$。若 $a'\equiv a(\mathrm{mon}\ p)$，则 $a=1$ 或 $p-1$。**

证明 由于 a 取值于 $\{1,2,\cdots,p-1\}$，$(a,p)=1$。方程 $ax\equiv 1 \pmod p$ 恰好有一个解 a'。假若 $a'\equiv b'(\mathrm{mon}\ p)$，在同余式两边同乘 ab，$aa'b\equiv ab'b \pmod p$。因 $aa'\equiv 1 \pmod p$，$bb'\equiv 1 \pmod p$，推出 $a\equiv b \pmod p$。从而当 $a\not\equiv b \pmod p$ 时，必有 $a'\not\equiv b' \pmod p$。又若 $a'\equiv a \pmod p$，同余式两边同乘 a，有 $a^2\equiv 1 \pmod p$。从引理 2.3 知 $a\equiv 1 \pmod p$ 或 $a\equiv p-1 \pmod p$。**证毕。**

定理 2.13 **（威尔逊定理）** **p 为素数当且仅当 $(p-1)!\equiv -1$**

(mod p)。

证明 p 是素数。当 $p=2$ 时，显然 $(2-1)!\equiv -1 \pmod 2$。当 $p>2$ 时。由引理 2.4 知 a 取值于集合 $\{2,3,\cdots,p-2\}$ 时，存在 $a'\neq a$ 且 $aa'\equiv 1 \pmod p$。当 a 取值不同时相应的 a' 也是不同的，从而 $2,3,\cdots,p-2$ 这 $p-3$ 个数可以把 a 与 a' 组成一对，即

$$2\cdot 3\cdots(p-2)\equiv 1 \pmod p;$$

$$(p-1)!=(p-1)\cdot 2\cdot 3\cdots(p-2)\equiv p-1\equiv -1 \pmod p.$$

反过来，已知 $(n-1)!\equiv -1 \pmod n$。令 a 是 n 的因子且 $a\neq n$。由 $n\mid(n-1)!+1)$，得到 $a\mid((n-1)!+1)$。显然 $a\mid(n-1)!$，于是 $a\mid 1$。由此推出 $a=1$。这说明 n 除了自身之外只有因子 1，n 是素数。

2.5 整数的因子及完全数

n 为正整数，$d(n)$ 表示 n 的正因子数，$\sigma(n)$ 表示 n 的正因子之和。显然

$$d(n)=\sum_{d\mid n}1,\qquad \sigma(n)=\sum_{d\mid n}d.$$

若 $n=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$，那么 $p_1^{f_1}\cdot p_2^{f_2}\cdots p_k^{f_k}$，$0\leqslant f_i\leqslant l_i$，$1\leqslant i\leqslant k$ 是 n 的正因子。每个 f_i 有 e_i+1 种不同的取值，从而 n 有 $(e_i+1)(l_2+1)\cdots(l_k+1)$ 个正因子，即

$$d(n)=(l_1+1)(l_2+1)\cdots(l_k+1).$$

$$\begin{aligned}
\sigma(n)&=\sum_{\substack{0\leqslant f_i\leqslant l_i\\ 1\leqslant i\leqslant k}}p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}.\\
&=\sum_{\substack{0\leqslant f_i\leqslant l_i\\ 1\leqslant i\leqslant k-1}}p_1^{f_1}p_2^{f_2}\cdots p_{k-1}^{f_{k-1}}\left(\sum_{f_k=0}^{l_k}p_k^{f_k}\right)\\
&=\sum_{\substack{0\leqslant f_i\leqslant l_i\\ 1\leqslant i\leqslant k-1}}p_1^{f_1}p_2^{f_2}\cdots p_{k-1}^{f_{k-1}}\left(\frac{p_k^{l_k+1}-1}{p_k-1}\right)\\
&\cdots\cdots\\
&=\frac{p_1^{l_1+1}-1}{p_1-1}\cdot\frac{p_2^{l_2+1}-1}{p_2-1}\cdot\cdots\cdot\frac{p_k^{l_k+1}-1}{p_k-1}.
\end{aligned}$$

不难看出，当$(m,n)=1$时，$\sigma(mn)=\sigma(m)\cdot\sigma(n)$，$d(mn)=d(m)\cdot d(n)$，即$d$和$\sigma$均是积性函数。

定义 2.7　正整数n为完全数当且仅当n等于除自身之外的正因子之和，即$\sigma(n)=2n$。

例如$6=1+2+3$，$28=1+2+4+7+14$，6与28是完全数。对于完全数已经得到了很好的结果。

定理 2.14　p为素数。如果2^p-1也是素数，则$2^{p-1}(2^p-1)$是完全数。

证明　p与2^p-1都是素数，由于$2^{p-1}<2^p-1$，知$(2^{p-1},2^p-1)=1$。σ是积性函数且

$$\sigma(2^{p-1})=\frac{2^p-1}{2-1}=2^p-1,\quad \sigma(2^p-1)=(2^p-1)+1=2^p.$$

$$\begin{aligned}\sigma(n)&=\sigma(2^{p-1}(2^p-1))=\sigma(2^{p-1})\sigma(2^p-1)\\&=(2^{p-1}-1)\cdot 2^p=2n,\end{aligned}$$

它说明$2^{p-1}(2^p-1)$是完全数，**证毕。**

定理 2.15　n是一个偶完全数，必有$n=2^{p-1}(2^p-1)$，其中p和2^p-1均为素数。

证明　n为偶完全数，可以表示成$n=2^k\cdot m$，其中$2\nmid m$，$k\geqslant1$。根据完全数的定义$\sigma(n)=2n$，即

$$2^{k+1}\cdot m=\sigma(2^k\cdot m)=\sigma(2^k)\sigma(m)=(2^{k+1}-1)\cdot(m+l).$$

解出$m=(2^{k+1}-1)\cdot l$。这里l是m的小于m的因子之和并且l本身也是m的因子，所以只能$l=1$。从而$m=2^{k+1}-1$，$\sigma(m)=m+1$。这说明m是素数。假设$k+1$不是素数，$k+1=c\cdot d$，$m=2^{k+1}-1=2^{c\cdot d}-1=(2^c-1)(2^{c(d-1)}+2^{c(d-2)}+\cdots+1)$，这与$m$是素数矛盾，故不可。$k+1$为素数$p$。综上分析知$n=2^{p-1}(2^p-1)$，其中$p$和$2^p-1$均是素数。**证毕**

形如2^p-1的素数叫作 Mersenne 数，直到 1985 年找到的最大 Mersenne 数为$2^{216091}-1$。

2.6 原根与指数

本节我们要解同余方程 $x^n \equiv c \pmod m$。当 $(c,m)=1$ 时，x_0 是 $x^n \equiv c \pmod m$ 的一个特解，而 y 是 $x^n \equiv 1 \pmod m$ 的解，则 $x \equiv yx_0 \pmod m$ 是 $x^n \equiv c \pmod m$ 的解。反过来 $x^n \equiv c \pmod m$ 的每个解都可以写成 yx_0 形式，其中 y 是 $x^n \equiv 1 \pmod m$ 的解。所以，解同余方程 $x^n \equiv c \pmod m$，只要找到一个特解 x_0，并用 x_0 乘以 $x^n \equiv 1 \pmod m$ 的全部解就得到了 $x^n \equiv c \pmod m$ 的全部解。

下面我们就来研究 $x^n \equiv 1 \pmod m$ 的解。为此引进阶，原根及指数的概念。

2.6.1 a 模 m 的阶

当 $(a,m)=1$ 时，考虑集合

$$A=\{n \mid n \in \mathrm{Z} \text{ 且 } a^n \equiv 1 \pmod m\},$$

由欧拉定理知 $\phi(m) \in A$ 且 $\phi(m)>0$。那么集合 A 中一定存在最小正整数 l。集合 A 显然有如下性质：

1° 若 n_1，$n_2 \in A$，则 $n_1 \pm n_2 \in A$。

2° 若 $n \in A$，$c \in \mathrm{Z}$，则 $cn \in A$。

3° 集合 A 是由 l 的整数倍数组成的，并且只有这些整数倍数组成的，即 $A=\{k \cdot l \mid k \in \mathrm{Z}\}$。

我们称 l 为 a 模 m 的阶。由集合 A 的性质知，当 $(a, m)=1$ 时，a 模 m 的阶为 l，那么对每个满足 $a^n \equiv 1 \pmod m$ 的整数 n 均有 $l \mid n$。特别地，$l \mid \phi(m)$。不难看出 $a^{n_1} \equiv a^{n_2} \pmod m$ 当且仅当 $n_1 \equiv n_2 \pmod l$。

推论 2.7 **若 $(a,m)=1$，l 为 a 模 m 的阶，则 a^k 模 m 的阶为 $\dfrac{l}{(l,k)}$。**

证明 首先看满足$(a^k)^j\equiv 1 \pmod m$的j应具有什么性质。从集合A的性质知$l\mid k\cdot j$，即

$$\frac{l}{(l,k)}\Bigg|\frac{k}{(l,k)}\cdot j,$$

由于$\left(\frac{l}{(l,k)},\ \frac{k}{(l,k)}\right)=1$，得到$\frac{l}{(l,k)}\mid j$. a^k的阶应是满足该性质最小的正整数，故a^k的阶为$\frac{l}{(l,k)}$. **证毕。**

2.6.2 原　　根

定义 2·8 **若$(g,m)=1$且g模m的阶为$\phi(m)$，则称g为模m的原根**

例如2是模5的原根，$\phi(5)=4$，$2^4\equiv 1 \pmod 5$。3是模7的原根，$\phi(7)=6$，$3^6\equiv 1 \pmod 7$。但并不是所有m都有原根。例如$m=8$，$\phi(8)=\phi(2^3)=4$. $\{1,3,5,7\}$是模8的缩系，而1模8的阶为1；3,5,7模8的阶为2。任何与8互素的数均与且仅与$\{1,3,5,7\}$中的一个元素模8同余，故其模8的阶与该元素相同。由此可知正整数8无原根。

取$0\leqslant i,j\leqslant\phi(m)-1$，$i\neq j$，显然$g^i\not\equiv g^j \pmod m$，$\{g^0,\ g^1,\ \cdots,\ g^{\phi(m)-1}\}$构成模$m$的缩系。也就是说，$g$是模$m$的原根，每个与$m$互素的$a$均与且仅与某个$g^i$模$m$同余，其中$0\leqslant i\leqslant\phi(m)-1$。模$m$的原根都在$\{g^0,\ g^1,\ \cdots,\ g^{\phi(m)-1}\}$中，若$(l,\phi(m))=1$，则$g^l$也是模$m$的原根。

下面接下去讨论哪些数有原根。其结论是所有的素数p都有原根，原根个数为$\phi(p-1)$。为此先给出两个引理。

引理 2.5 **若$f(x)$是n次整系数多项式，$f(x)\equiv 0 \pmod p$至多有n个解。**

证明 $f(x)$是n次整系数多项式，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，其中$a_n\not\equiv 0 \pmod p$. 对$f(x)$的次数$n$进行归纳证明。

当$n=1$时，$a_1x+a_0\equiv 0 \pmod p$且$a_1\not\equiv 0 \pmod p$，由定理

2.7 知该线性同余方程有唯一解。命题成立。假设 $n=k$ 时，$a_k x^k + a_{k-1}x^{k-1}+\cdots+a_0\equiv 0 \pmod p$ 至多有 k 个解。现 $n=k+1$。如果 $f(x)\equiv 0 \pmod p$ 无解，显然命题成立。如果 $f(x)\equiv 0 \pmod p$ 至少有一个解 r，即 $f(r)\equiv 0 \pmod p$。

$$
\begin{aligned}
f(x) &\equiv f(x)-f(r) \\
&= a_{k+1}(x^{k+1}-r^{k+1})+a_k(x^k-r^k)+\cdots+a_1(x-r) \\
&= (x-r)g(x) \pmod p,
\end{aligned}
$$

其中 $a_{k+1}\not\equiv 0 \pmod p$，$g(x)$ 是 k 次整系数多项式。$f(x)\equiv(x-r)g(x)\equiv 0 \pmod p$ 的任意解 s 使 $(s-r)g(s)\equiv 0 \pmod p$，即 $s\equiv r \pmod p$ 或 $g(s)=0 \pmod p$，也就是说 s 或是 r 或是 $g(s)\equiv 0 \pmod p$ 的解。由归纳假设知后者至多有 k 个解，所以 $f(x)$ 至多有 $k+1$ 个解。命题对 $n=k+1$ 也成立。**证毕。**

引理 2.6　若 $n\geqslant 1$，则 $\sum\limits_{d\mid n}\phi(d)=n$。

证明　由 $d\mid n$ 知 $\dfrac{n}{d}\Big| n$。故 $\sum\limits_{d\mid n}\phi(d)=\sum\limits_{d\mid n}\phi\left(\dfrac{n}{d}\right)$。

考虑集合 Cd，其中 d 是 n 的因子。

$$
\begin{aligned}
Cd &= \{m \mid 1\leqslant m\leqslant n \text{ 且 } (m,n)=d\} \\
&= \left\{m \,\middle|\, 1\leqslant m\leqslant n \text{ 且} \left(\frac{m}{d},\ \frac{n}{d}\right)=1\right\},
\end{aligned}
$$

显然 $|Cd|=\phi\left(\dfrac{n}{d}\right)$。$\{1,2,\cdots,n\}$ 中每个元素均在且仅在一个 Cd 中，从而

$$
n=\sum_{d\mid n}|Cd|=\sum_{d\mid n}\phi\left(\frac{n}{d}\right)=\sum_{d\mid n}\phi(d).
$$

证毕。

例如 $n=6$，n 的因子分别为 1，2，3，6。集合 $C_1=\{1,5\}$，$C_2=\{2,4\}$，$C_3=\{3\}$，$C_6=\{6\}$。

定理 2.16　p 为素数，$l\mid(p-1)$。那么模 p 阶为 l 的数恰好有 $\phi(l)$ 个。

证明　对于每个 $l\mid(p-1)$，令模 p 阶为 l 的元素个数记为

$\psi(l)$。如果对某个 l 不存在模 p 阶为 l 的元素，那么 $\psi(l)=0$。如果存在 a，a 与 p 互素且 a 模 p 阶为 l，即 $a^l\equiv1(\mathrm{mod}\ p)$。在集合$\{a^0, a^1, \cdots, a^{l-1}\}$中，由于各个元素的指数模 l 不同余，所以这些元素均模 p 不同余。而对于 $0\leqslant i\leqslant l-1$，

$$(a^i)^l=(a^l)^i\equiv1 \pmod p,$$

$a^0, a^1, \cdots, a^{l-1}$ 均是 $x^l\equiv1(\mathrm{mod}\ p)$的解。根据引理 2.5，该同余方程至多有 l 个解。这说明 $a^0, a^1, \cdots, a^{l-1}$ 是它的全部解，从推论 2.7 知 a^k 模 p 阶为 l 当且仅当$(k,l)==1$。$\{0,1,\cdots,l-1\}$ 中有 $\phi(l)$个与 l 互素的数，所以$\{a^0,a^1,\cdots,a^{l-1}\}$中有 $\phi(l)$个模 p 阶为 l 的数，即 $\psi(l)=\phi(l)$。综上知，对任何 $l|(p-1)$均成立 $\psi(l)\leqslant\phi(l)$。

另一方面，根据费尔马定理 $(a, p)=1$，$a^{p-1}\equiv1(\mathrm{mod}\ p)$。若 a 模 p 的阶为 t，则必有 $t|(p-1)$。满足该条件的 a 至少有 $p-1$ 个。由前面假设 $\psi(l)$是模 p 阶为 l 的元素个数。再由引理 2.6得到

$$\sum_{l|(p-1)}\psi(l)\geqslant p-1=\sum_{l|(p-1)}\phi(l)$$

并推出 $\psi(l)\geqslant\phi(l)$。

最后得到 $\psi(l)=\phi(l)$，即模 p 阶为 l 的数恰好有 $\phi(l)$个。**证毕。**

特别取 $l=\phi(p)$，模 p 阶为 $\phi(p)$的元素个数为 $\phi(\phi(p))=\phi(p-1)$。这说明有 $\phi(p-1)$个模 p 的原根。例如 37 是素数，它的原根数为

$$\begin{aligned}\phi(\phi(37))&=\phi(36)=\phi(2^2)\phi(3^2)\\&=2^1\cdot(2-1)\cdot3^1(3-1)=12.\end{aligned}$$

通过简单计算知 1 是 2 的原根，3 是 4 的原根，可以证明：m 有原根当且仅当 $m=2, 4, p^k, 2\cdot p^k$，其中 p 是奇素数，k 为正整数。再次说明 8 没有原根。

2.6.3 指　　数

设 g 为模 p 的原根，$\{g^0, g^1, \cdots, g^{p-2}\}$ 为模 p 的缩系。对每个整数 n，若 $(n, p)=1$，则存在 m，$0\leqslant m\leqslant p-2$ 使得 $n\equiv g^m \pmod p$ 成立。我们称 m 为 n（对于原根 g）的模 p 指数，并记为 $\operatorname{ind}_g n$。

若有 l 使 $n\equiv g^l \pmod p$，而 $n\equiv g^{\operatorname{ind}_g n} \pmod p$，所以 $l\equiv \operatorname{ind}_g n \pmod{p-1}$。

模 p 指数有如下性质：

1° $p\nmid ab$, $\operatorname{ind}_g ab\equiv \operatorname{ind}_g a+\operatorname{ind}_g b \pmod{p-1}$。

2° $p\nmid a$, $\operatorname{ind}_g a^l\equiv l\cdot \operatorname{ind}_g a \pmod{p-1}$。

这些性质从指数的定义很容易证出。不难看出模 p 指数与对数函数有相类似的性质。

定理 2.17　若 $(n,p)=1$，g 为模 p 的原根，则同余方程 $x^k\equiv n \pmod p$ 有解当且仅当 $(k, p-1)\mid \operatorname{ind}_g n$。当条件满足时，该方程有 $(k, p-1)$ 个解。

证明　令 $y=\operatorname{ind}_g x$，$x\equiv g^y \pmod p$ 代入 $x^k\equiv n \pmod p$，得到 $g^{yk}\equiv g^{\operatorname{ind}_g n} \pmod p$，即 $y^k\equiv \operatorname{ind}_g n \pmod{p-1}$。该方程有解 y 当且仅当 $(k, p-1)\mid \operatorname{ind}_g n$.并且条件满足时有 $(k, p-1)$ 个解。它们是

$$y\equiv y_1, y_2, \cdots, y_{(k,p-1)} \pmod{p-1}.$$

那么 $x\equiv g^{y_1}, g^{y_2}, \cdots, g^{y_{(k,p-1)}} \pmod p$ 是 $x^k\equiv n \pmod p$ 的解.证毕。

例 1　解同余方程 $x^8\equiv 3 \pmod{11}$。

解　查原根指数表知 11 的最小原根是 2，3 对于原根 2 的模 11 指数是 8。令 $y=\operatorname{ind}_2 x$，先解 $8\cdot y\equiv \operatorname{ind}_2 3=8 \pmod{10}$。因 $(8,10)=2$，该线性同余方程有 2 个模 10 不同余的解，它们是

$$y\equiv 1, 6 \pmod{10},$$

由此得到 $x\equiv 2^1, 2^6\equiv 2, 9 \pmod{11}$，它们是 $x^8\equiv 3 \pmod{11}$ 的

解.

例 2 解线性同余方程 $5x \equiv 7 \pmod{11}$

解 由 $5x \equiv 7 \pmod{11}$，以及 11 的最小原根为 2 知

$$\operatorname{ind}_2 5 + \operatorname{ind}_2 x \equiv \operatorname{ind}_2 7 \pmod{10}.$$

从原根指数表知 $\operatorname{ind}_2 5 = 4$，$\operatorname{ind}_2 7 = 7$，代入上式得到 $\operatorname{ind}_2 x \equiv 3 \pmod{10}$，故 $x \equiv 8 \pmod{11}$ 是原同余方程的解.

例 3 解同余方程 $x^8 \equiv 3 \pmod{143}$.

解 因 $143 = 11 \cdot 13$，要解 $x^3 \equiv 3 \pmod{143}$ 就是要解同余方程组

$$\begin{cases} x^8 \equiv 3 \pmod{11} \\ x^8 \equiv 3 \pmod{13}. \end{cases}$$

由例 1 知 $x^3 \equiv 3 \pmod{11}$ 的解为 $x \equiv 2, 9 \pmod{11}$. 用例 1 中的方法解出 $x^8 \equiv 3 \pmod{13}$ 的解为 $x \equiv 4, 6, 7, 9 \pmod{13}$.

下面求解

$$\begin{cases} x \equiv a \pmod{11} \\ x \equiv b \pmod{13}, \end{cases}$$

其中 $a = 2, 9$，$b = 4, 6, 7, 9$. 求解方法在 2.3.4 中已详述过，这里只给出结果 $x = 13 \cdot 6 \cdot a + 11 \cdot 6 \cdot b \pmod{143}$. 代入 a，b 的值，得到

$$x = \pm 9, \pm 20, \pm 35, \pm 46 \pmod{143}.$$

目前对给定素数 p 如何求出模 p 的原根尚无一般的方法. 另外，给定一个整数 a，它是哪些素数的原根也没有一般的方法. 在使用时可在一般的数论书中查到小素数的原根及相应的指数表. 表 1 给出 50 以内的素数的最小原根及相应的指数表. 该表中第一行列出 50 以内的全部素数 p，第一列是正整数 n. 素数 p 相应列中数值为 1 的元素对应的 n 值则是该素数的最小原根 g，该列的其它元素则是 $\operatorname{ind}_g n$.

表1 素数 $P(\leqslant 50)$ 的最小原根和指数表

n \ p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	26	27	18
3		3	1	8	4	1	13	16	5	1	26	15	1	20
4		2	4	2	2	12	2	4	2	18	2	12	12	36
5			5	4	9	5	16	1	22	20	23	22	25	1
6			3	9	5	15	14	18	6	25	27	1	28	38
7				7	11	11	6	19	12	28	32	39	35	32
8				3	3	10	3	6	3	12	3	38	39	8
9				6	8	2	8	10	10	2	16	30	2	40
10				5	10	3	17	3	23	14	24	8	10	19
11					7	7	12	9	25	23	30	3	30	7
12					6	13	15	20	7	19	28	27	13	10
13						4	5	14	18	11	11	31	32	11
14						9	7	21	13	22	33	25	20	4
15						6	11	17	27	21	13	37	26	21
16						8	4	8	4	6	4	24	24	26
17							10	7	21	7	7	33	38	16
18							9	12	11	26	17	16	29	12
19								15	9	4	35	9	19	45
20								5	24	8	25	34	37	37
21								13	17	29	22	14	36	6
22								11	26	17	31	29	15	25
23									20	27	15	36	16	5
24									8	13	29	13	40	28
25									16	10	10	4	8	2
26									19	5	12	17	17	29
27									15	3	6	5	3	14
28									14	16	34	11	5	22
29										9	21	7	41	35
30										15	14	23	11	39
31											9	28	34	3
32											5	10	9	44
33											20	18	31	27
34											8	19	23	34
35											19	21	18	33
36											18	2	14	30
37												32	7	42
38												35	4	17
39												6	33	31
40												20	22	9
41													6	15
42													21	24
43														13
44														43
45														41
46														23

习　　题

1. 证明：

(1) 若$a|b$，$a>0$，则$(a,b)=a$.

(2) $((a,b),b)=(a,b)$.

2. 证明：

(1) 对所有$n>0$成立$(n,n+1)=1$.

(2) 当$n>0$时，$(n,n+k)$可取什么值？

3. 求x和y使得

(1) $314x+159y=1$.

(2) $3141x+1592y=1$.

4. 证明：对于所有$n>0$，有$6|(n^3-n)$.

5. 证明：若对于某个m有$10|(3^m+1)$，则对所有$n>0$，$10|(3^{m+4n}+1)$.

6. 求2345及3456两个数的素数分解式.

7. 证明：当$n>0$时，$n(n+1)$决不会是一个平方数.

8. 令$n=5!+1$，证明$n+1$，$n+2$，$n+3$，$n+4$均为合数.

9. 求下列方程的所有整数解

(1) $x+y=2$.

(2) $2x+y=2$.

(3) $15x+16y=17$.

10. 求下列方程的负整数解

(1) $6x-15y=51$.

(2) $6x+15y=51$.

11. 用30张票面值为5分，1角，2角5分的纸币，换5元钱．问有多少种不同的兑换方法？

12. 某人用0.99元买了苹果和桔子共12个．每只苹果比每只桔子贵3分钱，买的苹果数多于桔子数．问他苹果和桔子各买多少个？

13. 若$k\equiv1\pmod 4$，问$6k+5$模4同余几？

14. 证明：每个大于3的素数模6或同余1或同余5.

15. 证明：相继的两个立方数之差决不能被3整除.

16. 证明：若一个整数的各位数字之和能被3整除，那么该数也能被3整除。

17. 证明：

(1) $10^k\equiv(-1)^k\pmod{11}$，$k=0,1,2,\cdots\cdots$

(2) 推出一个整数能被11整除的判别法.

18. 解下列线性同余方程：

(1) $2x\equiv1 \pmod{17}$.

(2) $3x\equiv6 \pmod{18}$.

(3) $4x\equiv6 \pmod{18}$.

(4) $3x\equiv1 \pmod{17}$.

19. 解下列同余方程组：

(1) $x\equiv1 \pmod 2$

$x\equiv1 \pmod 3$.

(2) $x\equiv31 \pmod{41}$

$x\equiv59 \pmod{26}$.

(3) $x\equiv1 \pmod 2$

$x\equiv1 \pmod 3$

$x\equiv6 \pmod 7$.

(4) $2x\equiv1 \pmod 5$

$3x\equiv2 \pmod 7$

$4x\equiv1 \pmod{11}$.

20. 试求同时满足如下两条要求的正整数 x，y，z.

(1) 它们分别乘以3，5，7所得乘积模20的余数是公差为1的算术级数.

(2) 它们分别乘以3，5，7所得乘积除以20得到的商分别等于(1)中相应的余数.

21. 求满足 $2|n$，$3|(n+1)$，$4|(n+2)$，$5|(n+3)$，$6|(n+4)$的最小整数 $n(>2)$.

22. 计算 $\phi(42)$，$\phi(420)$，$\phi(4200)$.

23. 小于18且与18互素的正整数是哪些？当 $m=18$，$a=5$时，验证引理2.1.

24. p为素数，$(m,n)=p$，问 $\phi(mn)$与 $\phi(m)\phi(n)$ 之间有什么关系？

25. 证明：

(1) 如果 $6|n$，则 $\phi(n)\leqslant\frac{n}{3}$.

(2) 如果 $n-1$ 和 $n+1$ 均为素数，$n>4$，则 $\phi(n)\leqslant\frac{n}{3}$.

26.

(1) 验证 $1+2=\frac{3}{2}\phi(3)$，$1+3=\frac{4}{2}\phi(4)$，$1+2+3+4=\frac{5}{2}\phi(5)$，$1+5=\frac{6}{2}\phi(6)$，$1+2+3+4+5+6=\frac{7}{2}\phi(7)$，$1+3+5+7=\frac{8}{2}\phi(8)$.

(2) 猜想一个定理.

(3) 证明你的定理.

27. 314^{159}除以7的余数是多少?

28. 7^{355}的末位数是什么? 末两位数是什么?

29. p为素数. 证明:对非负整数k, $(k+1)^p-k^p\equiv1 \pmod p$. 并由此推出费尔马定理.

30. 假设p是一个奇素数. 证明:

(1) $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv-1 \pmod p$.

(2) $1^p+2^p+\cdots+(p-1)^p\equiv0 \pmod p$.

31. 计算$d(42)$, $d(420)$, $d(4200)$, $\sigma(42)$, $\sigma(420)$, $\sigma(4200)$.

32. 求具有60个因子的数$n(n<10^4)$.

33. 证明

$$\sum_{d\mid n}\frac{1}{d}=\frac{1}{n}\sigma(n).$$

34. 证明所有的伸完全数以6或8结尾.

35. 若n为偶完全数, $n>6$, 证明$n\equiv1 \pmod 9$.

36. 证明

$$\sum_{p\leqslant x}\sigma(p)=\sum_{p\leqslant x}\phi(p)+\sum_{p\leqslant x}d(p).$$

37. 求2, 4, 7, 8, 11, 13, 14模15的阶是多少?

38.

(1) 算出关于原根2的最小指数表(mod 29).

(2) 利用此表解$9x\equiv2 \pmod{29}$.

(3) 利用此表解$x^9\equiv2 \pmod{29}$.

39. 问$457^{911}\equiv1 \pmod{10021}$对不对? (这里457, 911都是素数. $10021=11\cdot911$).

40. 求37的12个原根.

41. 证明: 若p, q为奇素数, $q\mid(a^p+1)$, 则有$q\mid(a+1)$或$q\mid2kp+1$, 其中k为某个整数.

42. 证明: 若a模p的阶为3, 则$a+1$模p的阶为6.

3 映　射

3.1 映射的基本知识

定义 3.1 设 A 和 B 是任意两个集合. 如果有一个确定的规律(或法则) f,它把集合 A 中的每个元素 a 都对应成集合 B 的唯一确定的元素 b, 则称这个规律(或法则) f 为从集合 A 到集合 B 的一个映射,表示成 $f: A\to B$ 或 $A \xrightarrow{f} B$.

定义 3.2 如果元素 $a\in A$ 经过映射 f 变成元素 $b\in B$, 则记成 $f(a)=b$ 或 $f: a\mapsto b$,称 b 为元素 a 在映射 f 之下的象, 或者叫做映射 f 在 a 点的值,而 a 叫 b 的原象.

从映射的定义看到,集合 A 中每个元素在映射 f 的作用下均有象并且象是唯一的.集合 B 中的元素可能没有原象. 集合 A 中的不同元素可能有相同的象,而集合 B 中的不同元素的原象必是集合 A 的不同元素.

如果 A 和 B 都是通常的数集合, 那么从集合 A 到集合 B 的映射就是普通的函数. 可见,映射的概念就是函数概念的推广. 若 A 本身是一个积集, $A=A_1\times A_2\times\cdots\times A_n$, f 是从集合 A 到集合 B 的映射,元素 $(a_1, a_2, \cdots, a_n)$其中 $a_i\in A_i$, $1\leqslant i\leqslant n$, 在映射 f 之下的象记为 $f(a_1, a_2, \cdots, a_n)\in B$, 它是相当普通的多元函数.

设 $f: A\to B$, $f(a)=b$. 我们说 $(a, b)\in f$.也就是说,把映射 f 看成是由全部原象与象构成的有序二数组组成的集合. 从而映射 f 是 $A\times B$ 的子集. 由于集合 A 中任意元素 a 的象是唯一的,

若 $(a, b)\in f$ 且 $(a, c)\in f$，则必有 $b=c$。

定义 3.3 $f: A\to B$，集合 A 的全部元素在映射 f 之下的全体象组成的集合称之为 f 的值域，记为 R_f。显然

$$R_f=\{b \mid b\in B,\ \text{存在 } a\in A \text{ 使 } f(a)=b\}\subseteq B.$$

定义 3.4 设 $f: A\to B$，$g: A\to B$。如果对任何 $a\in A$ 都有 $f(a)=g(a)$，则称映射 f 与 g 是相等的，记为 $f=g$。

例 1 $A=\{a_1, a_2, a_3, a_4\}$，$B=\{b_1, b_2, b_3\}$。若 $f(a_1)=f(a_3)=b_2$，$f(a_2)=f(a_4)=b_1$，则 f 是从集合 A 到集合 B 的映射，其值域 $R_f=\{b_1, b_2\}$。

例 2 $A=\{a_1, a_2, a_3\}$，$A=\{b_1, b_2, b_3\}$。若 $h(a_1)=b_1$，$h(a_1)=h(a_2)=b_2$，$h(a_3)=b_3$，则 h 不是从集合 A 到集合 B 的映射，这是因为它在 a_1 点的值不唯一。又若 $u(a_1)=u(a_2)=b_1$，则 u 也不是从集合 A 到集合 B 的映射，其原因是 A 中的元素 a_3 没有象。

有了定义 3.4 我们知道从集合 A 到集合 B 的映射怎样才是不同的。下面我们要计算从集合 A 到集合 B 可以定义多少个不同的映射。

定理 3.1 从有限集合 A 到有限集合 B 的映射共有 $|B|^{|A|}$ 个。

证明 A，B 是有限集合，$A=\{a_1, a_2, \cdots a_n\}$，$B=\{b_1, b_2, \cdots, b_m\}$，$|A|=n$，$|B|=m$。$f, g: A\to B$。$f$ 与 g 是从集合 A 到集合 B 的不同映射是指

$$(f(a_1), f(a_2), \cdots, f(a_n))\neq(g(a_1), g(a_2), \cdots, f(a_n)),$$

即至少存在一个 $1\leqslant i_0\leqslant n$，使 $g(a_{i_0})\neq g(a_{i_0})$。映射 f 在 $a_1, a_2, \cdots, a_n$ 点的取值是相互无关的，在每一点上的取值都是 B 集合中的任意一个元素，所以有 m 种可能性。从而 f 的取值方式共有 m^n 种。故从集合 A 到集合 B 的映射共有 $|B|^{|A|}$ 个。**证毕。**

例 1 令 $A=\{a_1, a_2\}$，$B=\{b_1, b_2, b_3\}$，从集合 A 到集合 B 的映射共有 $|B|^{|A|}=3^2=9$ 个，它们是

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9
a_1	b_1	b_1	b_1	b_2	b_2	b_2	b_3	b_3	b_3
a_2	b_1	b_2	b_3	b_1	b_2	b_3	b_1	b_2	b_3

而从集合 B 到集合 A 的映射共有 $|A|^{|B|}=2^3=8$ 个，它们是

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
b_1	a_1	a_2	a_1	a_2	a_1	a_2	a_1	a_2
b_2	a_1	a_1	a_2	a_2	a_1	a_1	a_2	a_2
b_3	a_1	a_1	a_1	a_1	a_2	a_2	a_2	a_2

3.2 特 殊 映 射

本节介绍几种具有特殊性质的映射。它们在以后各章节中起着重要作用。

定义 3.5 $f: A \to A$，对 A 中任意元素 a，均有 $f(a)=a$，称 f 为 A 上的恒同映射，记为 I_A。

定义 3.6 $f: A \to B$。如果 $R_f=B$，则称 f 为满射。

如果 $f(a_1)=f(a_2)$，必推出 $a_1=a_2$，则称 f 为单射。

如果 f 是满射且为单射，则称 f 为双射。

定义 3.7 若 f 是从集合 A 到集合 B 的双射，定义 $f^{-1}(b)=a$，如果 $f(a)=b$。那么 f^{-1} 称为映射 f 的逆映射。

令 $f: A \to B$，任取 A 的子集 S，定义 S 的象集

$$f(S)=\{f(x) \mid x \in S\}.$$

特别当 $S=\varnothing$ 时，$f(\varnothing)=\varnothing$，当 $S=A$ 时，$f(A)$ 叫映射 f 的象集，记为 $\mathrm{Im}\, f$。显然 $f: A \to f(A)$ 为满射。

定理 3.2 f 是从集合 A 到集合 B 的双射，如上定义的 f^{-1} 是从集合 B 到集合 A 的双射。

证明 从定义 3.7 知

$$f^{-1}=\{(b, a)|(a, b)\in f\}.$$

首先要说明如此定义的 f^{-1} 是从集合 B 到集合 A 的映射. 这是因为 f 是满射，集合 B 中的每个元素 b 均有 $a\in A$ 使 $(a, b)\in f$. 从而 $(b,a)\in f^{-1}$，即对于集合 B 中的每个元素 b 在 f^{-1} 的作用下均有象。又因 f 是单射，集合 B 中的每个元素 b 的原象是唯一的，所以集合 B 中的每个元素 b 在 f^{-1} 的作用下象是唯一的.

由于 f 是从 A 到 B 的映射，所以集合 A 的每个元素 a 一定出现在 $(a, b)\in f$ 中，从而每个 a 都出现在 $(b, a)\in f^{-1}$ 中. 也就是说 A 中的每个元素对于映射 f^{-1} 都有原象，所以 f^{-1} 是从 B 到 A 的满射.

设 $(b_1, a)\in f^{-1}$，$(b_2, a)\in f^{-1}$，有 $(a, b_1)\in f$. $(a, b_2)\in f$. 由于 f 是映射，元素 a 的象是唯一确定的，故 $b_1=b_2$. 也就是说，集合 A 的任意元素 a 对于映射 f^{-1} 的原象唯一，所以 f^{-1} 是从 B 到 A 的单射.

综上分析，知 f^{-1} 是双射. **证毕.**

定理 3.3 **A, B 是有限集合，存在着从 A 到 B 的满射的充要条件是 $|A|\geqslant|B|$.**

证明 设 f 是从 A 到 B 的满射，集合 B 中的每个元素都在集合 A 中对于映射 f 有原象. 而 B 中的不同元素的原象一定是不同的. 而且 B 中的元素 b 在 A 中的原象可能不只一个. 所以集合 A 中的元素个数一定大于集合 B 中的元素个数，即 $|A|\geqslant|B|$.

反过来，A, B 是有限集合，$A=\{a_1, a_2, \cdots, a_n\}$，$B=\{b_1, b_2, \cdots b_m\}$，$|A|\geqslant|B|$ 即 $n\geqslant m$. 定义 f: $A\to B$

$$f(a_i)=\begin{cases}b_i, & 1\leqslant i\leqslant m,\\ b_m, & m<i\leqslant n.\end{cases}$$

它是从 A 到 B 的满射. **证毕.**

定理 3.4 **A, B 是有限集合，如果存在着从集合 A 到集合 B 的双射，则 $|A|=|B|$.**

证明 设 f 是从 A 到 B 的双射，显然 f 也是从 A 到 B 的满射，由定理 3.3 知 $|A| \geqslant |B|$。f 的逆映射 f^{-1}，在定理 3.2 中已证明它是从 B 到 A 的双射，显然它也是从 B 到 A 的满射，同理得到 $|B| \geqslant |A|$。从而 $|A| = |B|$。**证毕。**

定理 3.5 两个 n 元集合间有 $n!$ 个不同的双射。

证明 A, B 是两个 n 元集合，$A = \{a_1, a_2, \cdots, a_n\}$，$B = \{b_1, b_2, \cdots, b_n\}$。$f$ 是从 A 到 B 的双射，它把 A 与 B 的元素之间建立了一种一对一的关系。f 在 a_1 点的值有 n 种选择，当确定 $f(a_1) = b_{i_1}$ 后，f 在 a_2 点的值就只有 $n-1$ 种选择，它只能取 $B - \{b_{i_1}\}$ 中的值。当确定 $f(a_2) = b_{i_2}$ 后，f 在 a_3 点的值有 $n-2$ 种选择，它只能取 $B - \{b_{i_1}, b_{i_2}\}$ 中的值。如此进行下去。当 f 在 a_{n-1} 点的值确定后，f 在 a_n 点的值只有唯一一种选择，不同的取值方式对应着不同的双射，所以从 A 到 B 有 $n!$ 个不同的双射。**证毕。**

例 1 设 $f(n) = 2n$ 是从整数集合到偶数集合的双射。它的逆映射是 $f^{-1}(2n) = n$。这里整数集合与偶数集合都是无限集合。所以可能存在双射把整数集合映到它的真子集偶数集合上。

例 2 R 为实数集合，$f: \mathrm{R} \times \mathrm{R} \to \mathrm{R}$，$f(x, y) = x \cdot y$。$f$ 是满射。由于 $f(3, 2) = f(1, 6) = 6$，所以 f 不是单射。

例 3 令 E 为万有集合，$\mathscr{P}(E)$ 是所有集合构成的集族。并运算 $\cup: \mathscr{P}(E) \times \mathscr{P}(E) \to \mathscr{P}(E)$。$\cup(A, B) = A \cup B$。任取 $A \in \mathscr{P}(E)$，$(\varnothing, A) \in \mathscr{P}(E) \times \mathscr{P}(E)$ $\cup$，$(\varnothing, A) = \varnothing \cup A = A$，$(\varnothing, A)$ 是 A 的原象，所以并运算是满射。而 $(A, \varnothing)$ 是 A 的另一个原象，所以并运算不是单射。

同理，交运算也具有相同的性质，而补运算是从 $\mathscr{P}(E)$ 到 $\mathscr{P}(E)$ 的双射。

例 4 A 是有限集合，$A = \{a_1, a_2, \cdots, a_n\}$，$B = \{0, 1\}$。对于 A 的每个子集 P 定义 $f(P) = (b_1, b_2, \cdots, b_n)$，其中

$$b_i = \begin{cases} 0 & a_i \notin P \\ 1 & a_i \in P, \end{cases} \quad 1 \leqslant i \leqslant n.$$

f 是集合 A 的幂集 $\mathscr{P}(A)$ 到集合 B^n 的一个映射并且是双射。

任取 B^n 的一个元素 $(b_1, b_2, \cdots, b_n)$，$b_i \in B$，$1 \leqslant i \leqslant n$。构造集合 $P = \{a_i | a_i \in A, b_i = 1\}$。显然 P 是 A 的子集，即 $P \in \mathscr{P}(A)$，并且

$$f(P) = (b_1, b_2, \cdots, b_n).$$

即 P 是 $(b_1, b_2, \cdots, b_n)$ 的原象。所以 f 是满射。

设 A 的子集 P_1 和 P_2 都是 $(b_1, b_2, \cdots, b_n)$ 的原象。那么从 $a_i \in P_2$ 推出 $b_i = 1$，从而 $a_i \in P_1$。反之亦然。所以 $P_1 = P_2$ 也就是说 B^n 中任意元素只有一个原象，即 f 是单射。综上得知 f 是从 $\mathscr{P}(A)$ 到 B^n 的双射。

3.3 映射的合成

设 $f: A \to B$，$g: B \to C$，$f(a) = b$，$g(b) = c$。那么连续执行 f 和 g 映射，它的总效果是把集合 A 的元素 a 映到集合 C 的元素 c。这就构成了一个新的映射。这个新的映射叫做 f 和 g 的合成映射，记为 $g \circ f$（图 2）。注意这里 f 写在右边表示先执行 f 映射再执行 g 映射。于是，对于 $a \in A$ 有

$$g \circ f(a) = g(f(a)).$$

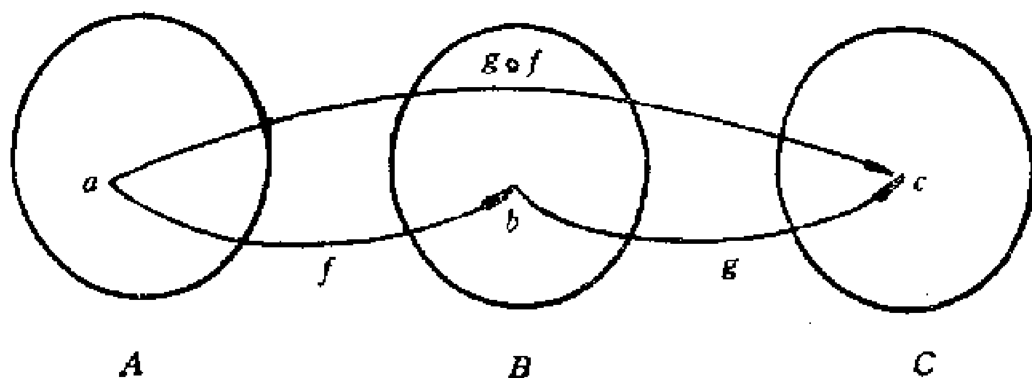


图 2

如果 A, B, C 都是通常的数集合，f, g 都是函数。那么上面叙述的合成映射就是通常的复合函数。

下面讨论合成映射的性质。

定理 3.6 如果映射 $f:A\to B$ 存在着逆映射 f^{-1}，那么 $f^{-1}\circ f=I_A$。

证明 $f: A\to B$，任取 $a\in A$，$f(a)=b\in B$。f 有逆映射那么 $f^{-1}(b)=a$。

$$f^{-1}\circ f(a)=f^{-1}(f(a))=f^{-1}(b)=a,$$

映射与其逆映射的合成映射为恒同映射，即 $f^{-1}\circ f=I_A$。**证毕。**

定理 3.7 映射的合成满足结合律。

证明 设 $f:A\to B$，$g:B\to C$，$h:C\to D$，要证明

$$(h\circ g)\circ f=h\circ(g\circ f).$$

首先看到 $(h\circ g)\circ f$ 与 $h\circ(g\circ f)$。都是从 A 集合到 D 集合的映射。任取 A 中元素 a，假设 $f(a)=b$，$g(b)=c$，$h(c)=d$，其中 $b\in B$，$c\in C$，$d\in D$。

$$(h\circ g)\circ f(a)=h\circ g\circ(f(a))=h\circ g(b)=h(g(b))=h(c)=d,$$

$$h\circ(g\circ f)(a)=h(g\circ f(a))=h(g(f(a)))=h(g(b))=h(c)=d,$$

得知 $(h\circ g)\circ f(a)=h\circ(g\circ f)(a)$。由 a 的任意性得到

$$(h\circ g)\circ f=h\circ(g\circ f).$$

证毕。

定理 3.8 设 $f:A\to B$，$g:B\to C$。

1° 若 f,g 是满射，则 $g\circ f$ 也是满射。

2° 若 f,g 是单射，则 $g\circ f$ 也是单射。

3° 若 f,g 是双射，则 $g\circ f$ 也是双射，并且 $g\circ f$ 的逆映射 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$。

证明 $f:A\to B$，$g:B\to C$ 的合成映射 $g\circ f:A\to C$。

1° 任取集合 C 的元素 c，因 $g: B\to C$ 是满射，存在 $b\in B$ 使 $g(b)=c$。而 $f:A\to B$ 是满射，存在 $a\in A$．使 $f(a)=b$。

$$g\circ f(a)=g(f(a))=g(b)=c.$$

a 就是元素 c 对于映射 $g\circ f$ 的原象，从而 $g\circ f$ 是满射。

2° 留作习题。

3° 由 1°, 2° 知 当 f,g 为双射时，$g\circ f$ 也是双射。下面证明 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$。

首先 $f:A\to B$, $g:B\to C$,则 $(g\circ f)^{-1}: C\to A$。而 $f^{-1}: B\to A$, $g^{-1}:C\to B$,则 $f^{-1}\circ g^{-1}: C\to A$。

任取集合 C 的元素 c，存在 $b\in B, a\in A$ 使 $g^{-1}(c)=b, f^{-1}(b)=a$。由合成映射的定义

$$f^{-1}\circ g^{-1}(c)=f^{-1}(g^{-1}(c))=f^{-1}(b)=a。$$

又计算 $g\circ f(a)=g(f(a))=g(b)=c$，知$(g\circ f)^{-1}(c)=a$。由元素 c 的任意性知

$$(g\circ f)^{-1}=f^{-1}\circ g^{-1}。$$

证毕。

3.4 置 换

本节介绍一种特殊的双射——有限集合上的双射，称之为置换。它在本课程以及组合数学中有很重要的作用。

3.4.1 置换的定义与性质

定义 3.8 A 是有限集合。从 A 到自身的双射称为集合 A 中的置换。若 $|A|=n$，则 A 中的置换称为 n 元置换。

$A=\{a_1, a_2, \cdots, a_n\}$,$n$ 元置换 σ 表示成

$$\sigma=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n)\end{pmatrix}, \quad \sigma(a_i)\in A,\ 1\leqslant i\leqslant n.$$

由于 σ 是 A 上的双射，$\sigma(a_i)\neq\sigma(a_j)$, $i\neq j$。特别，

$$\sigma_I=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n\end{pmatrix}$$

称为恒同置换。

例 1 $A=\{1,2,3,4,5\}$, $\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3\end{pmatrix}$，其中 $\sigma(1)$

$=2$, $\sigma(2)=5$, $\sigma(3)=1$, $\sigma(4)=4$, $\sigma(5)=3$.

在置换中，我们只关心集合 A 各元素相对位置的变化，并不关心元素本身。所以下面我们把 n 元集合都看成 $\{1, 2, \cdots, n\}$，一共有 $n!$ 个不同的 n 元置换。

前面讲过，双射存在逆映射，并且逆映射也是双射，对于置换 σ 必定存在逆置换 σ^{-1}。若

$$\sigma=\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

它的逆置换

$$\sigma^{-1}=\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & & n \end{pmatrix}.$$

例 2 求上例中 σ 的逆置换。

解

$$\sigma^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}^{-1}=\begin{pmatrix} 2 & 5 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}.$$

例 3 求 $A=\{1,2,3\}$ 上的全部置换。

解 $|A|=3$，A 上有 6 个不同的置换，它们是

$$\sigma_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\quad \sigma_2=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\quad \sigma_3=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_4=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\quad \sigma_5=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\quad \sigma_6=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

其中 σ_1 是恒同置换。

在置换 σ 中，如果 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 为奇排列（排列中逆序的个数为奇数），则称 σ 为奇置换。如果 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 为偶排列，则称 σ 为偶置换。例 1 中的 σ 里 25143 的逆序数为 5，所以 σ 是奇置换。例 3 中 σ_5 里 231 的逆序数为 2，所以 σ_5 是偶置换。

我们知道任何两个双射的合成映射仍是一个双射。两个置换 σ_i 和 σ_j 相继执行仍是一个置换。这个置换称为 σ_i 与 σ_j 的乘积，

记为 $\sigma_j\cdot\sigma_i$。在例 3 中

$$\sigma_4\cdot\sigma_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&3&2\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\sigma_6,$$

$$\sigma_2\cdot\sigma_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}3&2&1\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\sigma_5,$$

这里 $\sigma_4\cdot\sigma_2\neq\sigma_2\cdot\sigma_4$。由此看出，置换的乘法不满足交换律。

3.4.2 轮　换

轮换是一种特殊的置换。

定义 3.9　设 $a_1,a_2,\cdots,a_r$ 是集合 $A=\{1,2,\cdots,n\}$ 的 r 个不同的元素。σ 是 A 上的置换，它使 $\sigma(a_1)=a_2$，$\sigma(a_2)=a_3$，$\cdots$，$\sigma(a_{r-1})=a_r$，$\sigma(a_r)=a_1$，并且 A 中的其它元素 a 均有 $\sigma(a)=a$，即其它元素在 σ 的作用下保持不动。我们称 σ 是长为 r 的轮换，记作

$$\sigma=(a_1a_2\cdots a_r)。$$

称 a_1，a_2，$\cdots$，a_r 为轮换 σ 撤动的元素。

若 $\sigma=(a_1a_2\cdots a_r)$，则 $\sigma^{-1}=(a_ra_{r-1}\cdots a_1)$。例 3 中 $\sigma_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 2\ 3)$，$\sigma_5^{-1}=(3\ 2\ 1)=(1\ 3\ 2)=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\sigma_6$。

不难看出 $(a_1,a_2,\cdots a_r)=(a_2a_3\cdots a_ra_1)=\cdots=(a_ra_1\cdots a_{r-1})$。

轮换的乘积可用下面列表方式进行。例如 $\sigma=(1\ 3\ 4)$，$\tau=(1\ 2)$，

$$\sigma\cdot\tau=(1\ 3\ 4)(1\ 2)=(1\ 2\ 3\ 4)$$

$$\begin{array}{l} 2\longleftarrow 2\longleftarrow 1\\ 3\longleftarrow 1\longleftarrow 2\\ 4\longleftarrow 3\longleftarrow 3\\ 1\longleftarrow 4\longleftarrow 4 \end{array}$$

$$\tau\cdot\sigma=(1\ 2)(1\ 3\ 4)=(1\ 3\ 4\ 2)$$

$$\begin{array}{l} 3\longleftarrow 3\longleftarrow 1\\ 1\longleftarrow 2\longleftarrow 2\\ 4\longleftarrow 4\longleftarrow 3\\ 2\longleftarrow 1\longleftarrow 4 \end{array}$$

这里 $\sigma\cdot\tau\neq\tau\cdot\sigma$。

又若 $\sigma=(1\ 2)$，$\tau=(3\ 4)$，则 $\tau\cdot\sigma=\sigma\cdot\tau$。这是因为这两个轮换搬动元素集合的交为空，即它们没有共同搬动的元素的缘故。我们称这样的轮换是不相交的轮换．也就是说不相交的轮换乘积是可以交换的。

定理 3.9 每个置换都可以写成若干不相交的轮换之积。

证明 轮换只跟搬动了的元素有关系。我们对置换所搬动的元素个数进行归纳。

当置换只搬动两个元素，它们是 i 和 j，那么 $\sigma=(ij)$是长为 2 的轮换。命题成立。

假设置换搬动的元素个数小于m时，命题成立。现在置换 σ 搬动m个元素（$m\geqslant3$），σ 必定搬动了某个元素 i。由于 σ 是有限集合上的双射，序列 $i,\sigma(i),\sigma^2(i),\cdots,\sigma^k(i)$，…不可能两两互不相同，必存在 r，使 $\sigma^r(i)=i$。那么它们构成一个长为 r 的轮换 $\pi_0=(i,\ \sigma(i),\ \cdots,\ \sigma^{r-1}(i))$。现在观察 $\pi_0^{-1}\sigma$，原来 σ 不搬动的元素仍保持不动．$i,\ \sigma(i),\ \cdots,\ \sigma^{r-1}(i)$这 r 个元素也保持不动．从而 $\pi_0^{-1}\sigma$ 搬动元素个数小于 m。由归纳假设知 $\pi_0^{-1}\sigma=\pi_1\pi_2\cdots\pi_s$，其中 π_i，$\pi_j(i\neq j)$ 是两两互不相交的。而 $\sigma=\pi_0\pi_1\pi_2\cdots\pi_s$。这里 π_0 只搬动 $i,\sigma(i),\cdots,\sigma^{r-1}(i)$，而 $\pi_1,\pi_2,\cdots,\pi_s$ 不搬动 $i,\sigma(i),\cdots,$

$\sigma^{r-1}(i)$。所以 π_0 与 π_j，$1\leqslant j\leqslant s$ 是非交的。这就证明了命题对置换搬动 m 个元素时也成立。证毕。

这里要说明的是，如果不考虑轮换因子书写的顺序，那么任何置换表示成不相交的轮换之积其形式是唯一的。

例如

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&3&5&1&7&4&2&9&8\end{pmatrix}$$

$$=(1\ 6\ 4)(2\ 3\ 5\ 7)(8\ 9)。$$

σ 为置换，使 $\sigma^n=\sigma_I$ 的最小正整数 n 称为 σ 的阶。若 $\sigma=(a_1a_2\cdots a_r)$ 是长为 r 的轮换，那么 σ 的阶为 r。

定理 3.10　置换的阶等于它的轮换分解中各因子长度的最小公倍数。

证明　从定理 3.9 知置换 $\sigma=\pi_1\pi_2\cdots\pi_s$，其中 $\pi_1,\pi_2,\cdots,\pi_s$ 是两两互不相交的轮换，它们的阶分别为 $m_1,m_2,\cdots,m_s$。令 m 是 $m_1,m_2,\cdots,m_s$ 的最小公倍数，$m=[m_1,m_2,\cdots,m_s]$。显然

$$\sigma^m=\pi_1^m\pi_2^m\cdots\pi_s^m=\pi_1^{k_1m_1}\pi_2^{k_2m_2}\cdots\pi_s^{k_sm_s}=\sigma。$$

设 σ 的阶为 r，必有 $r\mid m$。

$$\sigma^r=\pi_1^r\pi_2^r\cdots\pi_s^r=\sigma_I。$$

由于 $\pi_1,\pi_2,\cdots,\pi_s$ 是两两互不相交的，必有 $\pi_i^r=\sigma_I$，$1\leqslant i\leqslant s$。而 π_i 的阶为 m_i 知 $m_i\mid r$，$1\leqslant i\leqslant s$。又推出 $m\mid r$。由整除的反对称性质，得出 $m=r$。证毕。

3.4.3 对　换

两个文字的轮换叫做对换。

任何轮换可以表示成对换的乘积

$$(a_1a_2\cdots a_r)=(a_1a_r)(a_1a_{r-1})\cdots(a_1a_3)(a_1a_2)。$$

由于每个置换可以表示成不相交的轮换之积，于是每个置换可以表示成对换之积。但是表示方法不唯一。例如

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix}$$
$$=(1\ 5)(1\ 2)(3\ 4)$$
$$=(1\ 3)(3\ 4)(4\ 5)(2\ 4)(1\ 4).$$
在两种分解中对换因子个数的奇偶性相同。

定理 3.11 对换是奇置换.

证明 在对换 (ij)中不妨假设 $i<j$,

$$(ij)=\begin{pmatrix}1&2\cdots&i-1&i&i+1&\cdots&j-1&j&j+1&\cdots&n\\1&2&i-1&j&i+1&\cdots&j-1&i&j+1&\cdots&n\end{pmatrix}.$$

下面一排数中逆序数为 $2\cdot(j-i)-1$。故对换是奇置换。

置换 $\sigma=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}$ 乘以特殊形式的对换 $(i\quad i+1)$得

$$\sigma(i\quad i+1)=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}(i\quad i+1)$$
$$=\begin{pmatrix}1&2&\cdots i-1&i&i+1&i+2&\cdots&n\\a_1&a_2&a_{i-1}&a_{i+1}&a_i&a_{i+2}&\cdots&a_n\end{pmatrix},$$

其效果是把原来置换中 a_i 与 a_{i+1} 交换位置. 如果 $a_i<a_{i+1}$, 逆序数增加 1, 如果 $a_i>a_{i+1}$,逆序数减少 1。总之, 逆序数的奇偶性发生变化。所以, 一个置换与形如$(i\ i+1)$ 的对换相乘得到的置换与原置换奇偶性相反。

一般形式的对换(ij),不妨假设 $i<j$.

$(i\ j)=(i\ i+1)(i+1\ i+2)\cdots(j-1\ j)(j-2\ j-1)\cdots(i\ i+1,)$
那么 $\sigma(i\ j)$将把 σ 的奇偶性改变 $2(j-i)-1$ 次,从而 $\sigma(i\ j)$与 σ 的奇偶性相反。

从上面的分析看出,奇置换分解成奇数个对换因子之积,偶置换分解成偶数个对换因子之积.

定理 3.12 全体 n 元置换中奇置换与偶置换各半,都有 $\frac{n!}{2}$ 个。

证明 全体 n 元置换共有 $n!$ 个。每个置换或者是奇置换或

者是偶置换，两者必居其一。令全体 n 元偶置换为集合 A_n，全体 n 元奇置换为集合 B_n。f 是从 A_n 到 B_n 的映射，对任何 $\sigma\in A_n$，$f(\sigma)=\sigma(12)$。任取 $\tau\in B_n$，$\tau(12)\in A_n$，

$$f(\tau(12))=\tau.$$

$\tau(12)$是 τ 的原象。f 为满射。又若 σ_1，$\sigma_2\in A_n$ 都是 $\tau\in B_n$ 的原象，即 $\sigma_1(12)=\sigma_2(12)$，推出 $\sigma_1=\sigma_2$。所以 f 为单射。从而 f 为从 A_n 到 B_n 的双射。由定理 3.4 知 $|A_n|=|B_n|$。因为 $|A_n\cup B_n|=n!$，$A_n\cap B_n=\varnothing$，所以 $|A_n|=|B_n|=\dfrac{n!}{2}$。

3.5 开关函数

3.5.1 定义和性质

令 $F_2=\{0,\ 1\}$，n 元开关函数 $f(x_1,\ x_2,\cdots,x_n)$ 是从 F_2^n 到 F_2 的映射。从定理 3.1 不难看出 n 元开关函数有 2^{2^n} 个。例如，二元开关函数共有 $2^{2^2}=16$ 个。它们是

x_1	x_2	f_0	f_1	f_2	$\cdots$	f_{14}	f_{15}
0	0	0	0	0		1	1
0	1	0	0	0	$\cdots$	1	1
1	0	0	0	1		1	1
1	1	0	1	0		0	1

其中函数 f_1 定义了两个布尔量之间逻辑乘运算，记为 $x_1\cdot x_2$。它的运算规则如下左图。

x_1	x_2	$x_1\cdot x_2$
0	0	0
0	1	0
1	0	0
1	1	1

x_1	x_2	x_1+x_2
0	0	0
0	1	1
1	0	1
1	1	1

只有当 x_1，x_2 都取值 1 时函数 $x_1 \cdot x_2$ 才取值 1。函数 f_7 定义了两个布尔量之间的逻辑加运算，记为 x_1+x_2。它的运算规则如上右图所示。只有当 x_1，x_2 都取值 0 时函数 x_1+x_2 才取值为 0。下面定义布尔量的逻辑补运算，它的运算规则是

x	$\bar{x}$
0	1
1	0

即函数 $\bar{x}$ 与 x 的取值相反。

定义 3.10 设 $f(x_1, x_2, \cdots, x_n)$ 与 $g(x_1, x_2, \cdots, x_n)$ 是 n 元开关函数。对 $(a_1, a_2, \cdots, a_n) \in F_2^n$ 定义

$$\bar{f}(a_1, a_2, \cdots, a_n) = \overline{f(a_1, a_1, \cdots, a_n)},$$

$$(f+g)(a_1, a_2, \cdots, a_n) = f(a_1, a_2, \cdots, a_n) + g(a_1, a_2, \cdots, a_n),$$

$$(f \cdot g(a_1, a_2, \cdots, a_n) = f(a_1, a_2, \cdots, a_n) \cdot g(a_1, a_2, \cdots, a_n),$$

称 $\bar{f}$ 为 f 的补函数。$f+g$，$f \cdot g$ 分别称为 f 与 g 的和函数与积函数。

例如 $f(x_1, x_2) = x_1 \cdot x_2$，$g(x_1, x_2) = x_2$。从下面真值表看出 $(f+g)(x_1, x_2) = x_2$，$(f \cdot g)(x_1, x_2) = x_1 \cdot x_2$，$\bar{f}(x_1, x_2) = \bar{x}_1 + \bar{x}_2$。

x_1	x_2	$\bar{x}_1$	$\bar{x}_2$	$\bar{x}_1+\bar{x}_2$	f	g	$\bar{f}$	$f+g$	$f \cdot g$
0	0	1	1	1	0	0	1	0	0
0	1	1	0	1	0	1	1	1	0
1	0	0	1	1	0	0	1	0	0
1	1	0	0	0	1	1	0	1	1

定理 3.13 设 f, g, h 是开关函数，那么

1° 结合律 $(f+g)+h = f+(g+h)$，

$(f \cdot g)g = f \cdot (g \cdot h)$。

2° 交换律 $f+g = g+f$，

$f \cdot g = g \cdot f$。

3° 分配律 $f+(g\cdot h)=(f+g)\cdot(f+h)$,

$f\cdot(g+h)=(f\cdot g)+(f\cdot h)$。

4° $f+0=f$,

$f\cdot 1=f$。

5° $f+\bar{f}=1$,

$f\cdot\bar{f}=0$。

证明 因 f,g,h 仅有两种可能的取值,采用“穷举法”可证明上述性质。例如:

f	g	h	$g+h$	$f\cdot(g+h)$	$f\cdot g$	$f\cdot h$	$f\cdot g+f\cdot h$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

$f\cdot(g+h)$ 与 $f\cdot g+f\cdot h$ 取值完全相同,故 $f\cdot(g+h)=f\cdot g+f\cdot h$。

证毕。

下面用定理3·13证明一些等式。

例 1 证明:$f+f=f$, $f\cdot f=f$。

证明

$f+f=(f+f)\cdot 1=(f+f)\cdot(f+\bar{f})=f+(f\cdot\bar{f})=f+0=f$.

$f\cdot f=(f\cdot f)+0=(f\cdot f)+(f\cdot\bar{f})=f\cdot(f+\bar{f})=f\cdot 1=f$.

例 2 证明:$f+1=1$, $f\cdot 0=0$.

证明

$f+1=f+(f+\bar{f})=(f+f)+\bar{f}=f+\bar{f}=1$.

$f\cdot 0=f\cdot(f\cdot\bar{f})=(f\cdot f)\bar{f}\cdot=f\cdot\bar{f}=0$。

例 3 如果 $f+g=1, f\cdot g=0$，则 $g=\bar{f}$。

证明 若 $g=\bar{f}$，显然 $f+g=1$，$f\cdot g=0$。如果函数 h 也满足 $f+h=1$，$f\cdot h=0$，那么

$$h=h\cdot 1=h\cdot(f+\bar{f})=h\cdot f+h\cdot\bar{f}=0+h\cdot\bar{f}=h\bar{f},$$

$$\bar{f}=\bar{f}\cdot 1=\bar{f}\cdot(f+h)=\bar{f}\cdot f+\bar{f}h=0+\bar{f}h=h\bar{f}.$$

从而 $h=\bar{f}$。这说明

$$\begin{cases} f+g=1 \\ f\cdot g=0 \end{cases}$$

的解存在且唯一，$g=\bar{f}$。

例 4 证明 $\overline{f+g}=\bar{f}\cdot\bar{g}$。

证明 我们的思路是先证明 $(f+g)\cdot(\bar{f}\cdot\bar{g})=0$，$(f+g)+(\bar{f}\cdot\bar{g})=1$，然后利用例 3 的结果得到 $\overline{f+g}=\bar{f}\cdot\bar{g}$。

$$\begin{aligned}(f+g)\cdot(\bar{f}\cdot\bar{g})&=(f\cdot(\bar{f}\cdot\bar{g}))+(g\cdot(\bar{f}\cdot\bar{g}))\\&=((f\cdot\bar{f})\cdot\bar{g})+((g\cdot\bar{g})\cdot\bar{f})\\&=(0\cdot\bar{g})+(0\cdot\bar{f})=0+0=0,\end{aligned}$$

$$\begin{aligned}(f+g)+(\bar{f}\cdot\bar{g})&=f+((g+\bar{f})\cdot(g+\bar{g}))\\&=f+((g+\bar{f})\cdot 1=f+(g+\bar{f})\\&=(f+\bar{f})+g=1+g=1.\end{aligned}$$

例 5 证明：$f+(f\cdot g)=f$，$f\cdot(f+g)=f$。

证明

$$f+(f\cdot g)=(f\cdot 1)+(f\cdot g)=f\cdot(1+g)=f\cdot 1=f$$

$$f\cdot(f+g)=(f+0)\cdot(f+g)=f+(0\cdot g)=f+0=f.$$

例 6 f,g,h 为 n 元开关函数，如果 $f\cdot g=f\cdot h$ 且 $f+g=f+h$，则 $g=h$。

证明 当 $g=1$ 时 $f\cdot 1=f\cdot h$。$f+1=f+h$。推出 $f=f\cdot h$，$1=f+h$。用 $\bar{f}$ 同时乘以 $1=f+h$ 两边，得到

$$\bar{f}=\bar{f}\cdot(f+h)=\bar{f}\cdot h.$$

而

$$h=h\cdot(f+\bar{f})=h\cdot f+h\cdot\bar{f}=hf+\bar{f}=f+\bar{f}=1.$$

当 $g=0$ 时，$f\cdot 0=f\cdot h, f+0=f+h$，推出 $f\cdot h=0, f=f+h$。用 $\bar{f}$ 同时乘以 $f=f+h$ 两边，得到

$$f\cdot\bar{f}=\bar{f}\cdot(f+h)=\bar{f}\cdot h,$$

即 $\bar{f}\cdot h=0$。而

$$h=h\cdot(f+\bar{f})=h\cdot f+h\cdot\bar{f}=0+0=0$$

我们看到 g 与 h 取值完全相同，故 $g=h$。

例 3，例 4，例 5 分别证明了 n 元开关函数的幂等律，摩尔根律和吸收律。这些性质今后都可以直接引用。

3·5·2 开关函数的小项表达式

通常一个开关函数可以有许多相互等价的表达方式。为了理论上研究的方便，需要一种标准的表达方式，使得每个开关函数有唯一的表达式，并且不同的开关函数有不同的表达式。下面介绍的小项表达式就是其中的一个方法。

对任意 n 元开关函数 $f(x_1, x_2, \cdots, x_n)$

$$f(x_1, x_2, \cdots, x_n)=x_1\cdot f(1, x_2, \cdots, x_n)+\bar{x}_1\cdot f(0, x_2, \cdots, x_n),$$

这是因为当 $x_1=0$ 时，等式右边为

$$0\cdot f(1, x_2, \cdots, x_n)+1\cdot f(0, x_2, \cdots, x_n)=f(0, x_2, \cdots, x_n),$$

而当 $x_1=1$ 时等式右边为

$$1\cdot f(1, x_2, \cdots, x_n)+0\cdot f(0, x_2, \cdots, x_n)=f(1, x_2, \cdots, x_n),$$

从而前面的等式成立。把这一等式应用到二元开关函数 $f(x_1, x_2)$ 上

$$\begin{aligned}f(x_1,x_2)&=x_1\cdot f(1,x_2)+\bar{x}_1\cdot f(0,x_2)\\&=x_1\cdot(x_2\cdot f(1,1)+\bar{x}_2 f(1,0))+\bar{x}_1(x_2\cdot f(0,1)\\&\quad+\bar{x}_2 f(0,0))\\&=f(1,1)x_1\cdot x_2+f(1,0)x_1\cdot\bar{x}_2+f(0,1)\bar{x}_1\cdot x_2\\&\quad+f(0,0)\bar{x}_1\cdot\bar{x}_2.\end{aligned}$$

把这一事实推广到 n 元开关函数有

$$f(x_1,x_2,\cdots,x_n)=\sum_{a_1,a_2,\cdots,a_n=0}^{1} f(a_1,a_2,\cdots,a_n)x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n},$$

其中

$$x^a=\begin{cases}1 & 当 x=a 时,\\ 0 & 当 x\neq a 时.\end{cases}$$

从而

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}=\begin{cases}1 & 当 x_1=a_1,x_2=a_2,\cdots,x_n=a_n 时,\\ 0 & 否则.\end{cases}$$

前面的公式就是 n 元开关函数 $f(x_1,x_2,\cdots,x_n)$ 的小项表达式. 其中 $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ 称为小项. n 元开关函数有 2^n 个不同的小项.

例 1 3 元开关函数 $f(x_1,x_2,x_3)$ 的真值表为

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

它的小项表达式为

$$\begin{aligned}f(x_1,x_2,x_3)&=f(0,0,0,)x_1^0x_2^0x_3^0+f(0,0,1)x_1^0x_2^0x_3^1\\&\quad+f(0,1,0)x_1^0x_2^1x_3^0+f(0,1,1)x_1^0x_2^1x_3^1\\&\quad+f(1,0,0)x_1^1x_2^0x_3^0+f(1,0,1)x_1^1x_2^0x_3^1\\&\quad+f(1,1,0)x_1^1x_2^1x_3^0+f(1,1,1)x_1^1x_2^1x_3^1\\&=\bar{x}_1\bar{x}_2x_3+\bar{x}_1x_2\bar{x}_3+\bar{x}_1x_2x_3+x_1\bar{x}_2x_3\\&\quad+x_1x_2x_3.\end{aligned}$$

例 2 求 $f(x_1,x_2,x_3)=x_1$ 的小项表达式.

解 $f(x_1, x_2, x_3) = x_1 \cdot (x_2 + \bar{x}_2)(x_3 + \bar{x}_3)$

$$= x_1x_2x_3 + x_1x_2\bar{x}_3 + x_1\bar{x}_2x_3 + x_1\bar{x}_2\bar{x}_3.$$

3.5.3 集合的特征函数

定义 3.11 E 为集合，$F_2=\{0,1\}$，对E的每个子集 $A\subseteq E$，定义一个函数 $\chi_A: E\to F$

$$\chi_A(x) = \begin{cases} 1 & \text{当 } x\in A, \\ 0 & \text{当 } x\notin A. \end{cases}$$

χ_A 称为集合 A 的特征函数。

显然，E 的不同子集对应着不同的特征函数。E 为有限集合时，E 的子集个数为 $2^{|E|}$。从 E 到 F_2 的映射个数也是 $2^{|E|}$。令 $g(A)=\chi_A$，g 是从 $\mathscr{P}(E)$到 $\{f|f: E\to F_2\}$ 的双射。

如果取 $E=F_2^n$，F_2^n的 2^{2^n} 个子集与从 F_2^n 到 F_2 的 2^{2^n} 个开关函数可以建立一一对应关系。对应的方法是：对于 $A\subseteq F_2^n$，A 的特征函数

$$\chi_A(x_1, x_2, \cdots x_n) = \begin{cases} 0 & \text{当 } (x_1, x_2, \cdots, x_n)\notin A \text{ 时}, \\ 1 & \text{当 } (x_1, x_2, \cdots, x_n)\in A \text{ 时}. \end{cases}$$

容易看出：若 A_1, A_2 的特征函数分别是 χ_{A_1}, χ_{A_2} 那么集合 $A_1\cap A_2$，$A_1\cup A_2$ 的特征函数是 $\chi_{A_1}\cdot\chi_{A_2}$，$\chi_{A_1}+\chi_{A_2}$。这样集合上的三种基本运算补(－)，交(∩)，并(∪)分别对应着开关函数的三种逻辑补，逻辑乘和逻辑加。把集合的运算规则与开关函数的运算规则加以比较，对它们的相似之处就不难理解了。这一点在第五章中将有进一步的叙述。

习 题

1．下列关系中哪些能构成映射，请说明理由．其中 N 为自然数集合，R 为实数集合．

(1) $\{(x_1, x_2)|x_1, x_2\in \mathrm{N}, x_1+x_2<10\}$．

(2) $\{(y_1, y_2)|y_1, y_2\in \mathrm{R}, y_2=y_1^2\}$．

(3) $\{(y_1, y_2) | y_1, y_2 \in \mathrm{R}, y_2^2 = y_1\}$

2. 令 $f: A \to B$，其中 $A = \{-1, 0, 1\}^2$，

$$f(x_1, x_2) = \begin{cases} 0, & x_1 \cdot x_2 > 0, \\ x_1 - x_2, & x_1 \cdot x_2 \leqslant 0. \end{cases}$$

(1) f 的值域 R_f 是什么？

(2) 从 A 到 R_f 有多少个不同的映射？

3. 下列函数中哪些是单射，满射和双射？说明理由．其中 Z 为整数集合，Z^+ 为正整数集合．

(1) $g: \mathrm{Z} \to \mathrm{Z}^+$．$g: n \mapsto |n| + 1$．

(2) $f: \mathrm{Z} \to \mathrm{N} \cup \{0\}$，$f(j) = j (\bmod 3)$．

($j (\bmod 3)$ 表示 j 除以 3 的非负余数)．

(3) $f: \mathrm{Z} \to \mathrm{Z}$，$f(n) = n + 1$，

$g: \mathrm{Z} \to \mathrm{Z}$，$g(n) = n - 1$，

(4) $f: \mathrm{N} \to \{0, 1\}$，$f(j) = \begin{cases} 0 & j \text{ 为奇数} \\ 1 & j \text{ 为偶数}, \end{cases}$

(5) $f: \mathrm{R} \to \mathrm{R}$，$f(j) = j^2 + 2j - 15$．

4. A，B 是有限集合．试给出一个从 $A \times B$ 到 $B \times A$ 的双射，并由此验证 $|A \times B| = |B \times A|$．

5. 令 $R[x]$ 表示全体实系数多项式．

(1) 证明：$\frac{\mathrm{d}}{\mathrm{d}x} f(x) = f'(x)$ 是从 $\mathrm{R}[x]$ 到 $\mathrm{R}[x]$ 的映射．它的值域是什么？是否为满射？是否为双射？

(2) 证明：$I(f(x)) = \int_0^x f(t) \mathrm{d}t$ 是从 $\mathrm{R}[x]$ 到 $\mathrm{R}[x]$ 的映射．它的值域是什么？是否为满射？是否为双射？

6. 设 $A = \{a_1, a_2, \cdots, a_n\}$，$|B| = m$，$S(B)$ 表示集合 B 中元素构成的全体有序 n 数组，即

$$S(B) = \{(b_{i_1}, b_{i_2}, \cdots, b_{i_n}) | b_{i_j} \in B, 1 \leqslant j \leqslant n\}$$

以 F 表示从 A 到 B 的映射全体．对于 F 中的每个映射 f，令

$$g(f) = (f(a_1), f(a_2), \cdots f(a_n),)$$

证明：g 是从 F 到 $S(B)$ 的双射，并由此证明从 A 到 B 的映射有 m^n 个．

7. 令 $\alpha: S \to T$，A 和 B 是 S 的子集合，证明

$$\alpha(A \cup B) = \alpha(A) \cup \alpha(B)$$

$$\alpha(A \cap B) \subseteq \alpha(A) \cap \alpha(B)\ .$$

给出一个例子说明 $\alpha(A \cap B) \neq \alpha(A) \cap \alpha(B)$．

8. 令 $\alpha: S \to T$，A 是 S 的子集，A 在 S 中的补 $\widetilde{A} = S - A$．当 α 是单射或满

射时，讨论 $\alpha(\tilde{A})$ 与 $\widetilde{\alpha(A)}$ 的关系。

9. f，g，h 是从 Z 到 Z 的映射，$f(x)=3x$，$g(x)=3x+1$，$h(x)=3x+2$，计算 $f\circ g$，$g\circ f$，$g\circ h$，$h\circ g$，$f\circ g\circ h$。

10. 令 f 是从 A 到 B 的单射。g 是从 B 到 C 的单射。证明 $g\circ f$ 是从 A 到 C 的单射。

11. 令 $s=\{1,2,3,\cdots\}$，给出两个从 S 到 S 的映射 f 和 g，使得 $f\circ g=I_s$，但是 $g\circ f\neq I_s$。如果 f 是双射，会发生什么情况?

12. 设

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix},$$

计算 $\tau\sigma$，$\tau^2\sigma$，$\sigma^2\tau$，$\sigma^{-1}\tau\sigma$。

13. 把下列置换写成不相交的轮换之积。

(1) (257)(78)(145).

(2) (72815)(21) (476)(12).

14. 把下列置换写成不相交的轮换之积。

(1) $\begin{pmatrix}1&2&3&4&5&6&7&8\\8&2&6&3&7&4&5&1\end{pmatrix}$.

(2) $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}$.

(3) $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&1&4&7&2&5&8&6\end{pmatrix}$.

15. 求下列置换的阶。

(1) (47) (261) (567) (1234).

(2) (163)(1357)(67)(12345).

16. 证明：任何 n 元置换可以表示成 (12)，(23)，…，($(n-1)$，n) 的乘积。

17. 求证下列恒等式：

(1) $x_1=x_1x_2x_3+x_1\bar{x}_2x_3+x_1x_2\bar{x}_3+x_1\bar{x}_2\bar{x}_3$.

(2) $x_1x_2+x_2x_3+x_3\bar{x}_1=x_1x_2+\bar{x}_1x_3$.

18. 如果 $f+g=g$，求证下面三个等式成立。

(1) $f\cdot g+\bar{f}=1$.

(2) $\bar{f}+g=1$.

(3) $f\cdot\bar{g}=0$.

19. 写出下列 2 元开关函数的小项表达式.

(1) 恒为 1 的函数.

(2) 当且仅当两个变量取值相同时函数值为 1.

4 二元关系

4.1 基本概念

4.1.1 关　　系

定义 4.1 $A_1, A_2, \cdots, A_n$ **是集合，** $A_1 \times A_2 \times \cdots \times A_n$ **的子集称为** $A_1 \times A_2 \times \cdots \times A_n$ **上的一个** n **元关系**R**。如果** $R=\varnothing$**，称** R **为空关系或平凡关系。如果** $R=A_1 \times A_2 \times \cdots \times A_n$**，则称** R **为万有关系。**

R 是 $A \times B$ 上的二元关系，也叫做从集合 A 到集合 B 的关系。R 的定义域为

$$\{x \mid x \in A, \exists y \in B, (x, y) \in R\}.$$

R 的值域为

$$\{y \mid y \in B, \exists x \in A, (x, y) \in R\}.$$

如果 $(a, b) \in R$，我们说 a 与 b 有关系 R，记为 aRb。如果 $(a, b) \notin R$，我们说 a 与 b 没有关系 R，记为 $a \not R b$。当 $A=B$ 时，R 称为 A 上的二元关系。

例 1 令 L 是整数集合 I 上的"小于关系"，因 $4<6$，$(4, 6) \in L$。而 $(6,4) \notin L$。

例 2 以自然数集合 N 作为万有集合。令 M 表示"…是…的倍数"关系。$4M2$，$2 \not M 4$。一般地，

$$xMy \Longleftrightarrow \exists k \in \mathrm{N} \text{ 使 } x=k \cdot y.$$

对所有 $x \in \mathrm{N}$ 均有 $0Mx$，$xM1$。若 $p \in \mathrm{N}$ 且 $p>1$，从 pMx 必推出 $x=1$ 或 $x=p$，那么 p 称为素数。如果 $x \not M 2$，则 x 为奇数。

例 3 实数集合上的二元关系可在笛卡尔平面上图示出来。

例如关系 R

$$R=\{(x,y)\mid |x|+|y|\leqslant 1\}.$$

它的图示是图 3 中划阴影的部分。

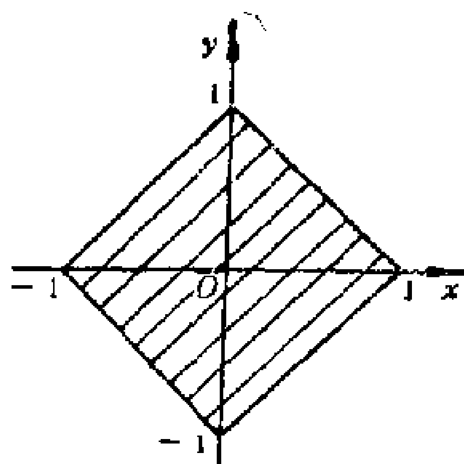


图 3

对比映射 $f: A\to B$ 和 $A\times B$ 上的二元关系 R,

$f=\{(x,y)\mid x\in A,\ y\in B,$ 并且 $f(x)=y\}$,

$R=\{(x,y)\mid x\in A,\ y\in B$ 并且 $xRy\}$.

f 的定义域 $D_f=A$,而 R 的定义域 $D_R\subseteq A$。在 f 中,如果 $(x,y_1)\in f$,$(x,y_2)\in f$ 必有 $y_1=y_2$.而在 R 中可能存在 $x_0\in A$,$y_1,y_2\in B$ 且 $y_1\neq y_2$ 使 $(x_0,y_1)\in R$,$(x_0,y_2)\in R$。所以,关系这个概念是从映射概念引伸出来的,它反映集合间的联系比映射还要广泛。

由于关系是集合.有些关系也可以采用归纳定义.例如:自然数集合上的"小于"关系的归纳定义如下:

1° (基础语句) $(0,1)\in R$。

2° (归纳语句)如果 $(x,y)\in R$,则 $(x,y+1)\in R$,$(x+1,y+1)\in R$。

3° (终结语句) R 只由有限次使用 1°,2° 所得到的那些元素组成。

4.1.2 关系的性质

定义 4.2 R 是 A 上的关系,

1° 如果对于 A 的每个元素 x 均有 xRx,则称 R 是自反的。

2° 如果对于 A 的每个元素 x 均有 $x\bar{R}x$,则称 R 是不自反的.

3° 对每个 $x,y\in A$,如果 xRy 必能推出 yRx,则称 R 是对称的。

4° 对每个 $x,y\in A$,如果 xRy,yRx 必能推出 $x=y$,则称

R 是反称对的。

5° 对每个 $x, y, z \in A$，如果 xRy，yRz 必能推出 xRz，则称 R 是传递的。

从这个定义看出如下两点：首先，一个关系 R 不具有"自反"性质，并不一定具有"不自反"性质。这两个性质不是互补的，这是因为可能集合 A 中的一些元素 x 使得 xRx 成立，而另一些元素 x 使 $x\not{R}x$ 成立。其次关系 R 的反对称性可等价地叙述成：如果 $x \neq y$ 且 xRy，则必有 $y\not{R}x$。

例 1 字母表 $\Sigma = \{a, b, \cdots, x, y, z\}$ 上定义的所有行组成的集合 Σ^* 上定义关系 R_1，R_2，R_3：

$xR_1y \Longleftrightarrow x$ 与 y 长度相等，

$xR_2y \Longleftrightarrow x$ 比 y 长，

$xR_3y \Longleftrightarrow x$ 的某个真前缀是 y 的一个真后缀。

R_1 是自反的，R_2 是不自反的，R_3 既不是自反的也不是不自反的这是因为 aaR_3aa 而 $ab\not{R}_3ab$。

例 2 在 Σ^* 上定义 R_4，R_5，R_6：

$xR_4y \Longleftrightarrow x$ 是 y 的子串，

$xR_5y \Longleftrightarrow x$ 与 y 都有一个相同的非空前缀，

$xR_6y \Longleftrightarrow x$ 与 y 相等。

R_4 是反对称的，R_5 是对称的，R_6 既是对称的也是反对称的。

例 3 在 Σ^* 上定义 R_7，R_8，R_9：

$xR_7y \Longleftrightarrow x$ 是 y 的前缀，

$xR_8y \Longleftrightarrow x$ 是 y 的子字，

$xR_9y \Longleftrightarrow x$ 与 y 有相同的字符。

R_7 和 R_8 都是传递的。R_9 不具有传递性，例如 abR_9bc，bcR_9cd，但是 $ab\not{R}_9cd$。

4.1.3 关系的表示

前面我们用集合形式表示 $A \times B$ 上的关系 R

$$R = \{(x, y) \mid x \in A, y \in B, xRy\}.$$

本节介绍另外两种关系的表示形式，即关系矩阵和关系图。

设 R 是从有限集合 A 到有限集合 B 的关系，其中 $A = \{a_1, a_2, \cdots, a_m\}$，$B = \{b_1, b_2, \cdots, b_n\}$。定义矩阵 $M = (m_{ij})$，

$$m_{ij} = \begin{cases} 0 \text{ 当 } & a_i \not R b_j \text{ 时}, \\ 1 \text{ 当 } & a_i R b_j \text{ 时}. \end{cases}$$

称为 R 的关系矩阵，它是 $m \times n$ 矩阵，即关系矩阵 M 的行数和列数分别是集合 A 和集合 B 的元素个数。

例 1 $A = \{a_1, a_2, a_3\}$，$B = \{b_1, b_2\}$。R 是 $A \times B$ 上的关系，

$$R = \{(a_1, b_1), (a_1, b_2), (a_2, b_2)\}.$$

R 的关系矩阵 M 是 3×2 矩阵，

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

例 2 R 是 $S = \{1, 2, 3, 4\}$ 上的关系，$xRy \Longleftrightarrow x \leqslant y$，$R$ 的关系矩阵 M 是 4 阶方阵。

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

从上面关系矩阵的构造方法看出：对于有限集合 A 上的关系 R，如果关系 R 是自反的，那么它所对应的关系矩阵 M 的对角线上所有元素都是 1。如果关系 R 是不自反的，那么关系矩阵 M 的对角线上所有元素都是 0。如果关系 R 是对称的，那么关系矩阵 M 是对称矩阵。如果关系 R 是反对称的，那么在关系矩阵 M 中 $i \neq j$ 且 $m_{ij} = 1$ 时，必有 $m_{ji} = 0$。或者说当 $i \neq j$ 时，$m_{ij} \cdot m_{ji} = 0$。关系 R 的传递性在关系矩阵中不易看出。

关系图表示法是把有限集合 $A = \{a_1, a_2, \cdots, a_n\}$ 上的关系 R 用一个有向图表示出来。其作法是：把集合 A 的每个元素用一个

点表示(称为结点)。如果 a_iRa_j,那么从结点 a_i 出发向结点 a_j 画一有箭头的弧。如果 a_iRa_i，则在结点 a_i 上画一条自封闭的弧线(称为圈)。

有限集合 A 上的任何关系都可以用关系图来表示。关系图直观地刻划出该关系的性质。如果关系 R 是自反的，那么关系图中每个结点都有一个圈。如果关系 R 是不自反的，那么每个结点都没有圈。如果关系 R 是对称的，a_i 与 a_j 是两个不同的结点，从 a_i 到 a_j 有条弧，那么从 a_j 到 a_i 也必有条弧。如果关系 R 是反对称的，两个不同结点 a_i 与 a_j 之间，从 a_i 到 a_j 有条弧，那么从 a_j 到 a_i 一定没有弧。如果关系 R 是传递的，从 a_i 到 a_j 有条首尾相接的弧串，那么从 a_i 到 a_j 一定有一条直接相连的弧（图 4)。

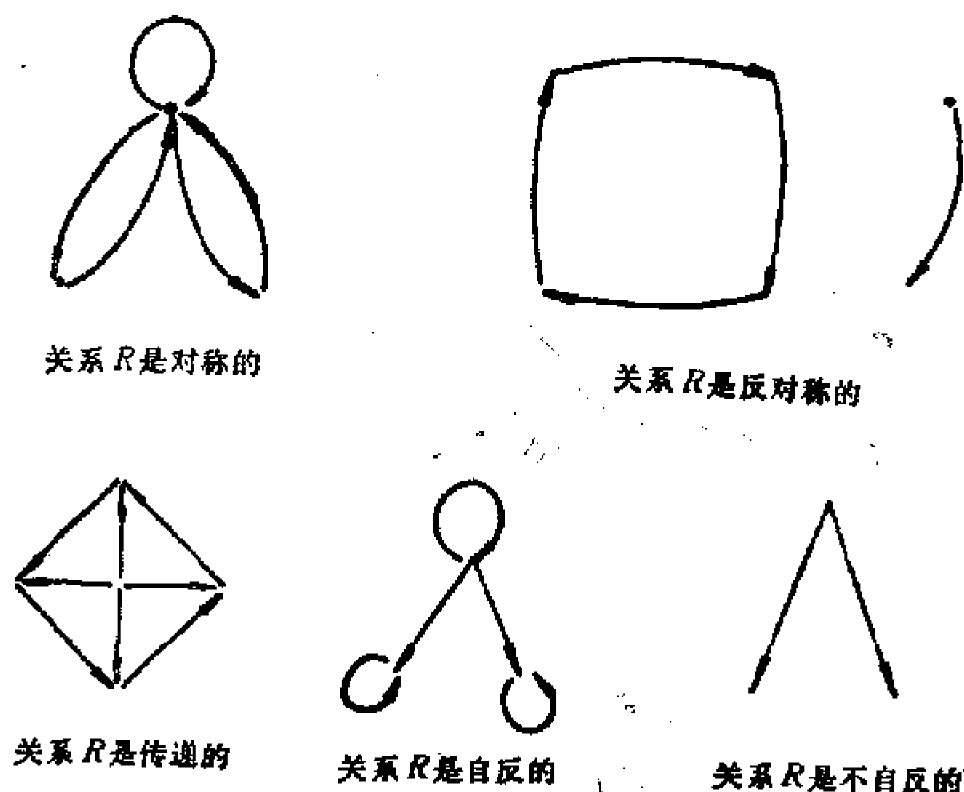


图 4

4.1.4 关系的运算

从集合 A 到集合 B 的关系 R，就是 $A\times B$ 的一个子集。集合之间的相等、包含以至于集合间的并、交、补运算可以直接地移植

到关系 R 上。

定义 4.3 ρ_1 **和** ρ_2 **是从集合** A **到集合** B **的两个关系。** ρ_1 **和** ρ_2 **作为** $A\times B$ **的子集而言，如果** $\rho_1\subseteq\rho_2$，**那么称关系** ρ_1 **小于等于关系** ρ_2，**并记为** $\rho_1\leqslant\rho_2$。

如果 $\rho_1\subseteq\rho_2$ **且** $\rho_1\neq\rho_2$，**则称关系** ρ_1 **小于关系** ρ_2，**并记为** $\rho_1<\rho_2$。

类似地可以定义$\geqslant$和$>$。

两个集合 A_1,A_2 满足 $A_1\subseteq A_2$，其含义是：若 $a_i\in A_1$，则必有 $a_i\in A_2$。两个关系 ρ_1,ρ_2 满足 $\rho_1\leqslant\rho_2$，可以刻划成，若 $x\rho_1y$，则必有 $x\rho_2y$。同样地，$\rho_1<\rho_2$ 可以刻划成，若 $x\rho_1y$，则必有 $x\rho_2y$，并且存在 $x_0\in A$，$y_0\in B$，使得 $x_0 \not\rho_1 y_0$ 且 $x_0\rho_2y_0$。

定义 4.4 ρ_1 **与** ρ_2 **是从集合** A **到集合** B **的两个关系。定义新的关系** $\rho_1\cap\rho_2$，$\rho_1\cup\rho_2$，$\bar{\rho}_1$ **为**

$$x(\rho_1\cap\rho_2)y\Longleftrightarrow x\rho_1y \text{ 且 } x\rho_2y,$$

$$x(\rho_1\cup\rho_2)y\Longleftrightarrow x\rho_1y \text{ 或 } x\rho_2y,$$

$$x\bar{\rho}_1y\Longleftrightarrow x \not\rho_1 y.$$

$\rho_1\cap\rho_2$，$\rho_1\cup\rho_2$，$\bar{\rho}$ 分别称为 ρ_1 与 ρ_2 的交、并及 ρ_1 的补。

例 1 ρ_1，ρ_2 是实数集合上的关系，它们的定义为 $x\rho_1y\Longleftrightarrow x=y$，$x\rho_2y\Longleftrightarrow x=-y$，那么

$$x(\rho_1\cup\rho_2)y\Longleftrightarrow |x|=|y|.$$

例 2 实数集合上的关系 ρ_1，ρ_2 定义为

$$x\rho_1y\Longleftrightarrow x\geqslant y,\quad x\rho_2y\Longleftrightarrow x\leqslant y,$$

那么

$$x(\rho_1\cap\rho_2)y\Longleftrightarrow x=y,$$

$$x\bar{\rho}_1y\Longleftrightarrow x<y.$$

集合间基本的运算（$\cup$，$\cap$，$\overline{}$）满足的运算规则可以原封不动地移到关系上。从而得到关系运算应该满足的运算规则，例如交换律 $\rho_1\cap\rho_2=\rho_2\cap\rho_1$，$\rho_1\cup\rho_2=\rho_2\cup\rho_1$；结合律 $(\rho_1\cup\rho_2)\cup\rho_3=\rho_1\cup(\rho_2\cup\rho_3)$，$(\rho_1\cap\rho_2)\cap\rho_3=\rho_1\cap(\rho_2\cap\rho_3)$，等等。

关系还有两个特殊的运算：合成运算和闭包运算。

定义 4.5 ρ_1 是从集合 A 到集合 B 的关系，ρ_2 是从集合 B 到集合 C 的关系。现从集合 A 到集合 C 的关系 $\rho_2\circ\rho_1$ 定义为

$$x(\rho_2\circ\rho_1)y \Longleftrightarrow \text{存在 } z\in B \text{ 使 } x\rho_1 z,\ z\rho_2 y,$$

并称为 ρ_1 和 ρ_2 的合成关系。

例 1 R, S 都是集合 $A=\{1, 2, 3, 4, 5\}$上的关系，其中

$$R=\{(1, 2), (2, 2), (3, 4)\},$$

$$S=\{(1, 3), (2, 5), (3, 1), (4, 2)\},$$

那么

$$R\circ S=\{(1, 4), (3, 2), (4, 2)\},$$

$$S\circ R=\{(1, 5), (2, 5), (3, 2)\}.$$

$R\circ S$ 及 $S\circ R$ 都是 A 上的关系，但是 $R\circ S\neq S\circ R$。可见合成运算是不满足交换律的。

定理 4.1 关系的合成运算满足结合律。

证明 设 R_1 是从集合 A 到集合 B 的关系，R_2 是从集合 B 到集合 C 的关系，R_3 是从集合 C 到集合 D 的关系。我们要证明 $R_3\circ(R_2\circ R_1)=(R_3\circ R_2)\circ R_1$。先证明 $R_3\circ(R_2\circ R_1)\subseteq(R_3\circ R_2)\circ R_1$。如果 $a\in A$, $d\in D$, $(a, d)\in R_3\circ(R_2\circ R_1)$，据据关系合成运算定义知存在 $c\in C$，使$(a, c)\in R_2\circ R_1$，$(c, d)\in R_3$。又由$(a, c)\in R_2\circ R_1$，根据合成运算定义知存在 $b\in B$，使$(a, b)\in R_1$，$(b, c)\in R_2$。我们把$(b, c)\in R_2$，$(c, d)\in R_3$ 放在一起，它的含义是存在 $c\in C$ 使得 $(b, c)\in R_2$ 且 $(c, d)\in R_3$，从而 $(b, d)\in R_3\circ R_2$。再把它与 $(a, b)\in R_1$ 结合在一起，知存在 $b\in B$，使得 $(a, b)\in R_1$且 $(b, d)\in R_3\circ R_2$，于是 $(a, d)\in(R_3\circ R_2)\circ R_1$。由此证明出 $R_3\circ(R_2\circ R_1)\subseteq(R_3\circ R_2)\circ R_1$。同理可证 $(R_3\circ R_2)\circ R_1\subseteq R_3\circ(R_2\circ R_1)$。由集合包含关系的反对称性得出

$$R_3\circ(R_2\circ R_1)=(R_3\circ R_2)\circ R_1.$$

证毕。

利用关系合成可以定义关系 R 的幂。$R^1=R$, $R^2=R\circ R$, $R^3=R^2\circ R=R\circ R^2$, …, $R^n=R^{n-1}\circ R=R\circ R^{n-1}$, …。由关系合成运算的

可结合性知对任何 $m>0$：

$$R^n=R^m\circ R^{n-m}.$$

定义 4.6　R 是集合 A 上的关系，如果有关系 R_1，它满足以下三条：

1° R_1 具有某种性质(如：自反性、传递性、对称性)。

2° $R\subseteq R_1$，

3° 对于任何具有该性质的关系 R_2，如果 $R\leqslant R_2$，则必有 $R_1\leqslant R_2$。

那么称 R_1 是 R 的该性质闭包。

由上面的定义看出，R 的某个性质闭包就是包含 R 且具有该性质的最小关系。

定理 4.2　R 是集合 A 上的关系，定义集合 A 上的关系 R^+，$a_1,a_2\in A$，

$$a_1R^+a_2\Longleftrightarrow \textbf{存在}\ n>0,\ a_1R^na_2.$$

R^+ 是关系 R 的传递闭包。

证明　首先证明 R^+ 是传递的。如果 $a,b,c\in A$，aR^+b，bR^+c，那么存在 $m,k>0$ 使 aR^mb，bR^kc。由合成关系的定义知 $aR^k\circ R^mc$，即 $aR^{k+m}c$。这说明 aR^+b，所以关系 R^+ 是传递的。

再证明 $R\leqslant R^+$。如果 $a,b\in A$，aRb，那么它就是 aR^1b。所以 aR^+b，从而 $R\leqslant R^+$。

最后证明 R^+ 是包含 R 的最小传递关系。不妨假设 P 是任意一个包含 R 的传递关系。如果 $c,b\in A$，aR^+b，那么存在着某个确定的 n，使 cR^nb。这就是说存在着 $n-1$ 个元素 $a_1,a_2,\cdots,a_{n-1}\in A$，使得

$$cRa_1,\ a_1Ra_2,\cdots,a_{n-2}Ra_{n-1},\ a_{n-1}Rb.$$

由于 $R\leqslant P$，显然

$$cPa_1,\ a_1Pa_2,\ \cdots,\ a_{n-2}Pa_{n-1},\ a_{n-1}Pb.$$

又由 P 的传递性知 cPb，从而 $R^+\leqslant P$。

综上分析，知 R^+ 是 R 的传递闭包。**证毕。**

定理4.3 R 是 A 上的关系，I_A 是 A 上的恒等关系（即对任何 $a\in A, aI_Aa$），$R'=I_A\cup R$ 是关系 R 的自反闭包。

定理4.4 R 是 A 上的关系，定义 A 上的关系 $\tilde{R}$

$$\tilde{R}=\{(y, x)\mid(x, y)\in R\}.$$

$R''=R\cup\tilde{R}$ 是 R 的对称闭包。

证明 由于 $R''=R\cup\tilde{R}\supseteq R$，显然 $R\leqslant R''$。如果 $a, b\in A$，$aR''b$，那么

$$\begin{aligned} aR''b &\Longleftrightarrow aRb \text{ 或 } a\tilde{R}b \\ &\Longleftrightarrow aRb \text{ 或 } bRa \\ &\Longleftrightarrow b\tilde{R}a \text{ 或 } bRa \\ &\Longleftrightarrow bR''a, \end{aligned}$$

R'' 是对称的。设 P 是包含 R 的对称关系。如果 $aR''b$，即 aRb 或 bRa，那么必有 aPb 或 bPa。由于 P 是对称关系，aPb 和 bPa 不管哪个成立都能推出 aPb。从而 $R''<P$。

综上分析知 R'' 是 R 的对称闭包。**证毕。**

4.2 等价关系

定义4.7 集合 A 上的自反、对称、传递关系叫做集合 A 上的等价关系。

R 是集合 A 上的等价关系。$a, b\in A$，如果 aRb，则称 a 与 b 等价，如果 aRb，由 R 的对称性知 bRa，那么我们称 a 与 b 彼此等价。由 R 的自反性知集合 A 中的每个元素 a 都与其自身等价。又由 R 的传递性知，如果 a 与 b 等价，b 与 c 等价，则 a 与 c 等价。

定义4.8 R **是集合 A 上的等价关系。对集合 A 中的每个元素 a 以 $[a]$ 表示 A 中与 a 等价的全体元素构成的集合，即**

$$[a]=\{x\mid x\in A, aRx\}.$$

由于 a 与 a 等价，$a\in[a]$，故 $[a]$ 称为元素 a 所属的等价类。

定理 4.5 R **是集合** A **上的等价关系，**

1° **对于集合** A **中的任意元素** a，b，**或者** $[a]=[b]$，**或者** $[a]\cap[b]=\varnothing$。

2° $\bigcup\limits_{a\in A}[a]=A$。

证明

1° 对于集合 A 中的任意元素 a 和 b，或者 aRb 或者 $a\not{R}b$，两者必居其一。

先看 aRb 的情况。由 R 的对称性知 bRa。任取 $x\in[a]$，显然 aRx。再由 R 的传递性得到 bRx，即 $x\in[b]$。由此得出 $[a]\subseteq[b]$。反过来，任取 $x\in[b]$，即 bRx。由 aRb 及 R 的传递性知 aRx，即 $x\in[a]$。又得出 $[b]\subseteq[a]$。根据集合包含关系的反对称性知 $[a]=[b]$。

再看 $a\not{R}b$ 的情况。如果 $[a]\cap[b]\neq\varnothing$，那么必存在 $x\in[a]\cap[b]$，即 $x\in[a]$ 且 $x\in[b]$。由等价类的定义知 aRx 且 bRx。再由 R 的对称性和传递性得到 aRb。这与前题发生矛盾，故不可。从而必有 $[a]\cap[b]=\varnothing$。

通过上面的讨论可知，彼此等价的元素属于同一个等价类，彼此不等价的元素所属的等价类没有公共元素。

2° 任取 $a_1\in\bigcup\limits_{a\in A}[a]$，元素 a_1 必是某个等价类的元素，不妨假设 $a_1\in[a_2]$。而 $[a_2]$ 是 A 的子集，故 $a_1\in A$。由此得出 $\bigcup\limits_{a\in A}[a]\subseteq A$。

反过来，任取 $a_1\in A$，显然 $a_1\in[a_1]\subseteq\bigcup\limits_{a\in A}[a]$。又得到 $A\subseteq\bigcup\limits_{a\in A}[a]$。

综上知 $A=\bigcup\limits_{a\in A}[a]$。**证毕。**

定义 4.9 A **是非空集合，集族** $\mathscr{A}=\{A_1, A_2, \cdots, A_k, \cdots\}$，**如果**

1° $A_i\subseteq A$，$1\leqslant i\leqslant k$。

2° $A_i \cap A_j = \varnothing$ 或者 $A_i = A_j$，$1 \leqslant i \neq j \leqslant k$。

3° $\bigcup_{i=1}^{k} A_i = A$。

则称 $\mathscr{A}$ 是集合 A 的一个划分。

不难看出，集合 A 上的等价关系 R 相应的等价类集合 $\{[a]_R \mid a \in A\}$ 是 A 的一个划分，它也称为 A 对于关系 R 的商集合。

例 1 Z 是整数集合。R_n 是 Z 上的模 n 同余关系，$x, y \in \mathrm{Z}$，

$$xR_ny \Longleftrightarrow n \mid (x-y) \Longleftrightarrow x \equiv y \pmod n.$$

我们在第二章中讲过，同余关系具有自反性，对称性和传递性，所以 R_n 是 Z 上的等价关系。$[0], [1], \cdots, [n-1]$ 是 R_n 所确定的全部等价类。

例 2 R 是复数集合 C 上的关系，$w, v \in \mathrm{C}$，$wRv \Longleftrightarrow |w| = |v|$。显然 R 是 C 上的等价关系。在复平面上以 O 点为圆心的圆上所有点在同一个等价类中。在图 5 中，以 O 点为圆心的所有同心圆是该等价关系确定的全部等价类。正实轴$[0, \infty)$称为它的代表元集合，这是因为每个等价类都有且仅有一个元素在该集合中。

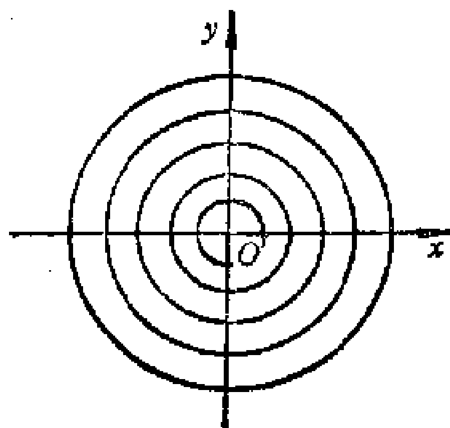


图 5

例 3 在平面几何中，若 A 是各种平面图形构成的集合。如果一个图形经过平移或旋转搬到另一图形上并彼此完全重合，那么就称这两个几何图形"全等"。这种"全等"关系是等价关系。彼此全等的几何图形构成一个等价类。

如果一个几何图形经过成比例地放大缩小而变成另一个图形，那么就称这两个几何图形是"相似"的。几何图形的相似关系也是等价关系。彼此相似的几何图形构成一个等价类。例如所有的圆都属于同一个相似等价类。

前面说过，由等价关系可以确定集合的一个划分。反过来，给定一个集合的划分也能确定对应该划分的一个等价关系。

定理 4.6 A **是非空集合，** $\mathscr{A}=\{A_1, A_2, \cdots, A_k, \cdots\}$ **是** A **的一个划分。定义集合** A **上的关系** R，$x, y\in A$，

$$xRy \Longleftrightarrow \text{存在一个 } i\text{，使 } x\in A_i \text{ 并且 } y\in A_i\text{，}$$

则关系 R 是集合 A 上的等价关系。

证明 $\mathscr{A}=\{A_1, A_2, \cdots, A_k, \cdots\}$ 是集合 A 的一个划分，$A=\bigcup_{i=1}A_i$。对任意 $x\in A$，必然存在一个 i 使 $x\in A_i$，从 R 的定义知 xRx，即 R 是自反的。如果 $x, y\in A$，xRy，即存在一个 i 使 $x\in A_i$ 并且 $y\in A_i$。于是 yRx，R 是对称的。又如果 $x, y, z\in A$，xRy，yRz，即存在 i 和 j 使 $x\in A_i$，$y\in A_i$，$y\in A_j$，$z\in A_j$，那么 $y\in A_i\cap A_j$，$A_i\cap A_j$ 是非空的。而 $\mathscr{A}$ 是 A 的一个划分，从而推出 $A_i=A_j$。由 $x\in A_i$，$z\in A_i=A_j$ 得到 xRz。R 是传递的。

综上分析知 R 是集合 A 上的等价关系，它所确定的等价类集合为 $\mathscr{A}$，证毕。

在一个集合上用不同方式定义的两种等价关系可能会产生同一个划分。例如 $A=\{1, 2, \cdots, 9\}$。在 A 上定义关系 R_1 和 R_2：

$$xR_1y \Longleftrightarrow 3\mid(x-y)\text{，}$$

$$xR_2y \Longleftrightarrow x \text{ 与 } y \text{ 在矩阵 } B \text{ 的同一列中，}$$

其中

$$B=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix}.$$

R_1 和 R_2 均是集合 A 上的等价关系，它们的等价类为

$$[1]=\{1, 4, 7\}，[2]=\{2, 5, 8\}，[3]=\{3, 6, 9\}.$$

这时我们称 $R_1=R_2$。这是因为“划分”的概念与“等价关系”的概念本质上是相同的。

4.3 序 关 系

序关系是另外一类重要的关系。

4.3.1 部 分 序

定义 4.10 集合 A 上的自反、反对称、传递关系叫作集合 A 上的部分序关系，或叫部分序。集合 A 和它上的一个部分序 ρ 构成部分序集，记作 $\langle A, \rho\rangle$。

例 1 实数集合 R 上的 $\leqslant$ 和 $\geqslant$ 关系都是部分序。$\langle \mathrm{R}, \leqslant\rangle$ 和 $\langle \mathrm{R}, \geqslant\rangle$ 是部分序集。

例 2 在万有集合 E 的幂集 $\mathscr{P}(E)$ 上 $\subseteq$ 和 $\supseteq$ 关系都是部分序。$\langle \mathscr{P}(E), \subseteq\rangle$ 和 $\langle \mathscr{P}(E), \supseteq\rangle$ 是部分序集。

R 是集合 A 上的部分序，a 与 b 是 A 中的两个元素。如果 aRb，则称 a 与 b 是可比较的。由 R 的自反性知 A 中的每个元素与其自身是可比较的。由 R 的反对称性知，如果 a 与 b 是可比较的，b 与 a 也是可比较的，那么必有 $a=b$。由 R 的传递性知，如果 a 与 b 是可比较的，b 与 c 是可比较的，那么 a 与 c 是可比较的。

一般说来，集合 A 中任取两个元素，它们不一定是可以比较的。例如集族 $\mathscr{P}(E)$ 上的 $\subseteq$ 关系是部分序。随便取两个集合，它们不一定有包含与被包含关系，为此引进线性序的概念。

4.3.2 线 性 序

定义 4.11 ρ 是集合 A 上的部分序。如果 A 中任意两个元素 a 和 b 都是可比较的，即 $a\rho b$ 或 $b\rho a$ 至少有一个成立，那么称 ρ 是线性序或完全序。$\langle A, \rho\rangle$ 称为线性序集。

前面例 1 中的 $\langle \mathrm{R}, \leqslant\rangle$ 和 $\langle \mathrm{R}, \geqslant\rangle$ 是线性序集。

$\langle A, \rho\rangle$ 是线性序集。我们用 $a\tilde{\rho}b$ 表示 $a\rho b$ 且 $a\neq 0$。现在 A^*

中定义 ρ'。$a_i, b_j \in A$，$1 \leqslant i$，$j \leqslant n$，$(a_1, a_2, \cdots, a_n)\ \rho'\ (b_1, b_2, \cdots, b_n)$ 当且仅当下面三个条件之一成立：

1° $(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$。

2° $a_1 \tilde{\rho} b_1$。

3° 存在自然数 t，$1 \leqslant t \leqslant n-1$，使 $a_i = b_i$，$1 \leqslant i \leqslant t$，而 $a_{t+1} \tilde{\rho} b_{t+1}$。

下面证明 ρ' 是 A^n 上的部分序。

首先由 1° 知 ρ' 是自反的。其次，如果$(a_1, a_2, \cdots, a_n)\rho'(b_1, b_2, \cdots, b_n)$，那么从定义中的 1°，2°，3° 都可以推出 $a_1 \rho b_1$。同理，如果 $(b_1, b_2, \cdots, b_n)\rho'(a_1, a_2, \cdots, a_n)$，推出 $b_1 \rho a_1$。由 ρ 的反对称性知 $a_1 = b_1$。如此证明下去，推出 $a_2 = b_2, \cdots, a_n = b_n$，即 $(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$。所以 ρ' 是反对称的。最后证明 ρ' 是传递的。如 $(a_1, a_2, \cdots, a_n)\rho'(b_1, b_2, \cdots, b_n)$ 且 $(b_1, b_2, \cdots, b_n)\rho'(c_1, c_2, \cdots, c_n)$，要证明 $(a_1, a_2, \cdots, a_n)\rho'(c_1, c_2, \cdots, c_n)$。因为 $(a_1, a_2, \cdots, a_n)\ \rho'(b_1, b_2, \cdots, b_n)$，定义中的 1°，2°，3° 必有其中一条成立。而 $(b_1, b_2, \cdots, b_n)\rho'(c_1, c_2, \cdots, c_n)$，下面的 (1)，(2)，(3) 中必有一条成立：

(1) $(b_1, b_2, \cdots, b_n) = (c_1, c_2, \cdots, c_n)$。

(2) $b_1 \tilde{\rho} c_1$。

(3) 存在自然数 v，$1 \leqslant v \leqslant n-1$，使 $b_i = c_i$ $1 \leqslant i \leqslant v$，而 $b_{v+1} \tilde{\rho} c_{v+1}$。

如果 1° 成立再加上 $(b_1, b_2, \cdots b_n)\rho'(c_1, c_2, \cdots, c_n)$，则推出$(a_1, a_2, \cdots, a_n)\rho'(c_1, c_2, \cdots, c_n)$。如果 2° 成立，即 $a_1 \tilde{\rho} b_1$。又由 $(b_1, b_2, \cdots, b_n)\rho'(c_1, c_2, \cdots, c_n)$，不管 (1)，(2)，(3) 哪条成立都有 $b_1 \tilde{\rho} c_1$，那么可以推出 $a_1 \tilde{\rho} c_1$，从而 $(a_1, a_2, \cdots, a_n)\rho'(c_1, c_2, \cdots, c_n)$。同理，如果 (1) 或 (2) 成立，再加上 $(a_1, a_2, \cdots, a_n)\rho'(b_1, b_2, \cdots, b_n)$ 也可以推出同样的结论。因此只剩下 3° 和 (3) 成立的情况。假设 3° 和 (3) 成立，且 $t \geqslant v+1$，那么 $a_i = b_i = c_i$，$1 \leqslant i \leqslant v$，且 $a_{v+1} = b_{v+1}$ 而 $b_{v+1} \tilde{\rho} c_{v+1}$，从而 $a_{v+1} \tilde{\rho} c_{v+1}$，即$(a_1, a_2, \cdots,$

$a_n)\rho'(c_1, c_2, \cdots, c_n)$。而当 3° 和 (3) 成立，且 $t \leqslant v+1$ 时，$a_i = b_i = c_i, 1 \leqslant i \leqslant t$，且 $b_{t+1} = c_{t+1}, a_{t+1}\tilde{\rho} b_{t+1}$。从而 $a_{t+1}\tilde{\rho} c_{t+1}$，即$(a_1, a_2, \cdots, a_n)\rho'(c_1, c_2, \cdots, c_n)$。

这就证明了 ρ' 是 A^n 上的部分序。实际上 ρ' 是 A^n 上的线性序。也就是说 A^n 中的任意两个元素 $(a_1, a_2, \cdots, a_n)$ 和 $(b_1, b_2, \cdots, b_n)$都是可比较的。这只要把有序 n 数组从左到右每个元素逐个比较即可。比较的过程是：如果 $a_1 \neq b_1$，因 ρ 是线性序，必有 $a_1\tilde{\rho} b_1$ 或者 $b_1\tilde{\rho} a_1$。那么就相应得出$(a_1, a_2, \cdots, a_n)\rho'(b_1, b_2, \cdots, b_n)$ 或者$(b_1, b_2, \cdots, b_n)\rho'(a_1, a_2, \cdots, a_n)$。如果 $a_1 = b_1$，那么我们就接下去比较第二个元素 a_2 和 b_2。一般地，如果 $a_1 = b_1$，$a_2 = b_2, \cdots, a_t = b_t$ $(t < n)$而 $a_{t+1} \neq b_{t+1}$，那么 $a_{t+1}\tilde{\rho} b_{t+1}$ 和 $b_{t+1}\tilde{\rho} a_{t+1}$ 两者必居其一，从而$(a_1, a_2, \cdots, a_n)\rho'(b_1, b_2, \cdots, b_n)$或者$(b_1, b_2, \cdots, b_n)\rho'(a_1, a_2, \cdots, a_n)$。最后如果两个有序 n 数组每对元素都相等，即 $(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$。这时仍有 $(a_1, a_2, \cdots, a_n)\rho'(b_1, b_2, \cdots, b_n)$。

在 A^n 上如此定义的线性序 ρ' 称为字典序。它在计算机科学中是一个重要的序关系。

4.3.3 极大元与极小元

定义 4.12 $\langle A, \rho\rangle$ **为部分序集，$x, y \in A$。如果 $x\tilde{\rho} y$，并且在 A 中不存在元素 z 使得 $x\tilde{\rho} z$，$z\tilde{\rho} y$，则称元素 y 控制元素 x，或者说元素 x 被元素 y 所控制，记作 $x\mathring{\rho} y$。**

在部分序集中，不是每个元素都控制着某个其它元素，也不是每个元素都被别的元素所控制。例如：部分序集 $\langle \mathrm{R}, \leqslant\rangle$ 中，每个元素都不控制别的元素，并且每个元素也不被其它元素所控制。

定理 4.7 **当 A 是有限集合时，对于 A 中的元素 a，如果有 $b \in A$ 使得 $a\tilde{\rho} b$，那么必然存在 b'，使 $a\mathring{\rho} b'$，即 a 的控制元素一定存在。**

证明 $\langle A,\rho\rangle$为部分序集，$a\in A$，存在$b\in A$且$a\tilde{\rho}b$。这里有两种可能性：b是a的控制元素，$a\mathring{\rho}b$。取$b'=b$即可；b不是a的控制元素，那么存在$b_1\in A$，$b_1\neq b$使$a\tilde{\rho}b_1$，$b_1\tilde{\rho}b$。这里仍然有两种可能性：b_1是a的控制元素$a\mathring{\rho}b_1$，取$b'=b_1$即可；b_1不是a的控制元素，存在$b_2\neq b_1$使$a\tilde{\rho}b_2$，$b_2\tilde{\rho}b_1$。不难看出$b_2\neq b$（如若$b_2=b$，那么$b_2\tilde{\rho}b_1$变成$b\tilde{\rho}b_1$，再加上$b_1\tilde{\rho}b$。由ρ的反对称性知$b_1=b$。这与$b_1\neq b$矛盾，故不可）。

如果我们一直找不到元素a的控制元素，上述过程就可以无限地进行下去，得到无限序列$\{b_1, b_2, \cdots, b_n, \cdots\}$，其中$b_i\in A$并且$a\tilde{\rho}\cdots$，$b_n\tilde{\rho}b_{n-1}$，$b_{n-1}\tilde{\rho}b_{n-2}$，$\cdots$，$b_3\tilde{\rho}b_2$，$b_2\tilde{\rho}b_1$，$b_1\tilde{\rho}b$，这里$b_1$，$b_2$，$\cdots$，$b_n$，$\cdots$是两两互不相同的。这就与$A$是有限集合相矛盾。于是上述过程就应该使$a\tilde{\rho}b_i$成立且$b_i$是$a$的控制元素。**证毕。**

从这个定理可以看出，对有限集合A上的序关系ρ，A中的每个元素a或者没有元素b使$a\tilde{\rho}b$，或者a存在控制元素。

同理，$\langle A,\rho\rangle$为部分序集，A为有限集合，A中每个元素a或者没有元素b使$b\tilde{\rho}a$，或者a控制某个元素。

例 1 $Z=\{1, 2, 3, 4, 6, 12\}$。Z_1上的整除关系是部分序关系。元素1的控制元素为2，3。元素2的控制元素为4，6。元素3的控制元素为6。元素4和6的控制元素为12。元素12没有控制元素。

定义 4.13 **$\langle A,\rho\rangle$是部分序集，对于集合A中的元素a，如果不存在元素b使得$a\tilde{\rho}b$，则称a为部分序集的极大元。**

如果不存在元素b使得$b\tilde{\rho}a$，则称a为部分序集的极小元。

根据定理4.7，每个有限部分序集可以绘成一个图表（称为Hasse图）。它直观地把序关系表示出来，对我们深入研究部分序集的结构带来方便。在这个图表中，最上方是极大元，最下方是极小元。其余每个元素向上用线段连至它的全部控制元素，向下用线段连至它的全部被控制元素。

例 2 $A=\{1, 2, 3\}$。部分序集$\langle\mathscr{P}(A), \subseteq\rangle$的Hasse图为

图 6，{1，2，3} 是极大元，$\varnothing$ 是极小元。

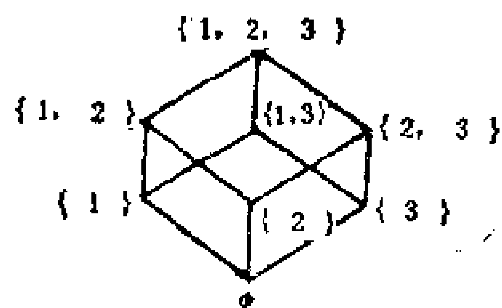


图 6

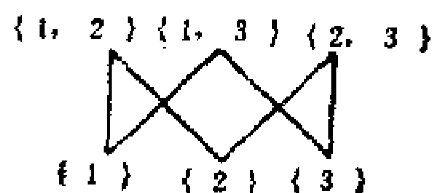


图 7

例 3 ⟨{{1}，{2}，{3}，{1，2}，{2，3}，{1，3}}，⊆⟩ 是部分序集，它的 Hasse 图为图 7。{1，2}，{2，3}，{1，3} 都是极大元，{1}，{2}，{3} 都是极小元。

例 4 $B=\{1,2,3,5,6,10,15,30\}$。B 与其上的整除关系构成部分序集⟨B，|⟩，它的极大元是 30，极小元是 1。其 Hasse 图为图 8。

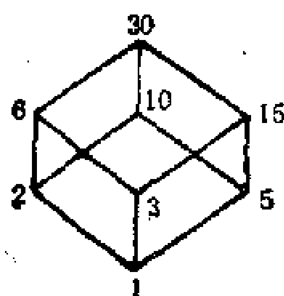


图 8

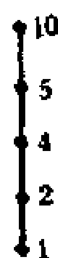


图 9

例 2 与例 4 中的两个部分序集有形状相同的 Hasse 图。这表明 ⟨$\mathscr{P}(A)$，⊆⟩ 与 ⟨B，|⟩ 尽管具体含义不同，但是它们的序结构完全相同。我们把有相同 Hasse 图的两个部分序集称为是序同构的。

例 5 ⟨{1，2，4，5，10}，≤⟩ 是部分序集，它的 Hasse 图是一条链（图 9）。不难看出，有限序集是一个线性序集当且仅当它的 Hasse 图是一条链。

4.3.4 最大元与最小元

定义 4 $\langle A, \rho\rangle$ **是部分序集。若集合 A 中的元素 x_0 对于 A 中的每个元素 y 均有 $y\rho x$，则称 x 为 $\langle A, \rho\rangle$ 的最大元。**

若对 A 中每个元素 y 均有 $x\rho y$，则称 x 为最小元。

前面例 2 中 $\{1, 2, 3\}$ 是最大元，$\varnothing$ 是最小元。例 3 中无最大元和最小元。例 4 中 30 是最大元，1 是最小元。例 5 中 10 是最大元，1 是最小元。

下面分析最大元与极大元的关系。

定理 4.8 **部分序集 $\langle A, \rho\rangle$ 的最大元必是极大元。**

证明 用反证法。令 x 是部分序集 $\langle A, \rho\rangle$ 的最大元。假设它不是 $\langle A, \rho\rangle$ 的极大元，从极大元的定义知必存在 $y\in A$，$x\tilde{\rho}y$。即 $x\neq y$ 且 $x\rho y$。由于 x 是 $\langle A, \rho\rangle$ 的最大元。对于 $y\in A$，必有 $y\rho x$。再从 ρ 的反对称性推出 $x=y$，这与 $x\neq y$ 矛盾，故不可，所以部分序集的最大元必是极大元。证毕。

定理 4.9 部分序集 $\langle A, \rho\rangle$ 的最大元至多有一个。

证明 部分序集不一定有最大元。如果 $\langle A, \rho\rangle$ 有最大元，并且假设 $x_1, x_2\in A$ 都是最大元，那么根据最大元的定义．x_1 是最大元，对于 A 中每个元素 x，特别取 $x=x_2$ 有 $x_2\rho x_1$。又 x_2 也是最大元，对于 A 中每个元素 x，特别取 $x=x_1$ 有 $x_1\rho x_2$。再由 ρ 的反对称性推出 $x_1=x_2$。这说明当 $\langle A, \rho\rangle$ 有最大元时．最大元只能有一个。证毕。

定理 4.10 **A 为有限集合，部分序集 $\langle A, \rho\rangle$ 存在最大元，当且仅当 $\langle A, \rho\rangle$ 只有一个极大元。**

证明 令 x 是 $\langle A, \rho\rangle$ 的最大元，根据定理 4.8 知 x 是 $\langle A, \rho\rangle$ 的极大元。假若除此之外 $\langle A, \rho\rangle$ 还有一个极大元 $x_0(\neq x)$。由于 x 是最大元，应 $x_0\rho x$，并推出 $x_0\tilde{\rho}x$。这与 x_0 是极大元矛盾，故不可。也就是说 $\langle A, \rho\rangle$ 只有一个极大元。

反过来，令 x 是 $\langle A, \rho\rangle$ 的唯一极大元，我们要证明 x 必是 $\langle A,$

$\rho\rangle$的最大元。任取集合 A 的元素 $y(\neq x)$，因 y 不是极大元，必存在 $y_1\in A$ 使 $y\tilde{\rho}y_1$。有两种情况：若 $y_1=x$，显然得到 $y\rho x$。若 $y_1\neq x$，那么 y_1 也不是极大元，从而存在 $y_2\in A$ 使 $y_2\tilde{\rho}y_1$（显然（$y_2\neq y$）。这时又有两种情况：若 $y_2=x$，那么从 $y\tilde{\rho}y_1$，$y_1\tilde{\rho}y_2$ 知 $y\rho x$。若 $y_2\neq x$，那么 y_2 也不是极大元，存在 $y_3\in A$，使 $y_2\tilde{\rho}y_3$（显然 $y_3\neq y_1$，$y_3\neq y$），…这样一直分析下去，得到 y_1，y_2，y_3，…。它们是两两互不相同的元素。由于 A 是有限集合，这一过程不可能无限地进行下去，而是到某步要终止。也就是说，存在 i，$y_i\rho y_{i+1}$ 且 $y_{i+1}=x$。于是，从

$$y\tilde{\rho}y_1,\ y_1\tilde{\rho}y_2,\ \cdots,\ y_{i-1}\tilde{\rho}y_i,\ y_i\tilde{\rho}x$$

推出 $y\rho x$。由 y 的任意性以及最大元的定义知 x 是 $\langle A,\ \rho\rangle$ 的最大元。

综上分析，证明了部分序集 $\langle A,\rho\rangle$ 存在最大元当且仅当 $\langle A,\rho\rangle$ 只有一个极大元。**证毕。**

用同样方法可以讨论最小元与极小元的关系并得出类似的结论。

4.3.5 上界与下界

定义 4.15 $\langle A,\rho\rangle$ **为部分序集。**M **是** A **的子集。**a **是** A **中的一个元素。如果对于** M **中的任意元素** m**，都有** $m\rho a$**，则称** a **是子集** M **的上界。**

如果对于 M **中的任意元素** m**，都有** $b\rho m$**，**$b\in A$**，则称** b **为** M **的下界。**

集合 A 的任意子集 M 不一定有上界或下界。即使有上界或下界也不一定唯一。例如 $\langle\{1, 2, 3, 4, 5, 6\}, |\rangle$ 是部分序集，它的 Hasse 图为图 10。最小元是 1，无最大元。4，5，6 是极大元。子集 $\{1, 2, 4\}$ 的上界为 4，子集 $\{1, 3\}$ 的上界为 3 和 6，子集 $\{3, 4\}$ 无上界。

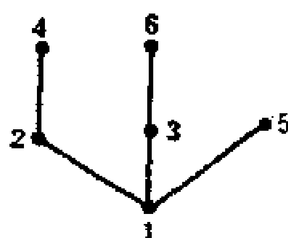


图 10

一般的上界和下界对我们研究问题作用不大，人们往往关心的是最小上界和最大下界。它们定义如下：

定义 4.16 **$a\in A$ 是 A 的子集 M 的上界，如果对于子集 M 的每个上界 x 均有 $a\rho x$，则称 a 为 M 的最小上界**

$b\in A$ 是 A 的子集 M 的下界，如果对于子集 M 的每个下界 x 均有 $x\rho b$，则称 b 为 M 的最大下界。

4.4 集合的势

集合的势是用来度量集合规模大小的属性的。对于有限集合，可用集合的元素个数来进行度量，对于无限集合这个办法就行不通了。为此我们需要采用一种新的方法来比较两个集合规模的大小。这种方法应该对有限集合和无限集合都适用。

定义 4.17 **如果存在着从集合 A 到集合 B 的双射，那么称集合 A 与集合 B 等势，记为 $A\sim B$。**

例 1 集合 $N=\{0, 1, 2, \cdots\}$，$N_2=\{0, 2, 4, \cdots\}$。定义映射 $f: N\to N_2$，$f(n)=2n$。f 是从 N 到 N_2 的双射。从而 N 和 N_2 是等势的。

E 是万有集合，$\mathscr{P}(E)$ 是所有集合构成的集族。集合间的等势关系是 $\mathscr{P}(E)$ 上的一个等价关系，这是因为任取 $A\in\mathscr{P}(E)$，存在双射 $f: A\to A, f(a)=a$，即 $A\sim A$。等势关系具有自反性。如果 $A, B, C\in\mathscr{P}(E)$，$A\sim B$，$B\sim C$，即存在双射 f，g，其中 $f: A\to B$，$g: B\to C$，那么合成映射 $g\circ f: A\to C$ 仍为双射，故 $A\sim C$。等势关系是传递的。如果 A，$B\in\mathscr{P}(E)$，$A\sim B$，即存在双射 $f: A\to B$，那么 f 的逆映射 $f^{-1}: B\to A$ 仍为双射，故 $B\sim A$。等势关系是对称的。综上知等势关系是 $\mathscr{P}(E)$ 上的等价关系。

利用等势关系可以把所有集合进行等价分类，那么在一个等价类里面的集合是等势的。

4.4.1 有限集合与可数集合

定义 4.18 与一个自然数集合的断片 $[0, n] = \{0, 1, 2, \cdots, n\}$ 等势的集合叫做有限集合。空集 $\varnothing$ 也是有限集合。不是有限集合的集合叫做无限集合。

如果集合 A 与 $[0, n]$ 等势，则存在双射 $f: [0, n] \to A$，$f(i) = a_i$，即 $A = \{a_0, a_1, a_2, \cdots, a_n\}$是有限集合，并且可以逐个地把它的全部元素枚举出来，因此有限集合的势可以用它的元素个数来表示。空集的势为 0。

任何有限集合不能与它的真子集等势。这是因为 A, B 为有限集合且 $A \subset B$，则必有 $|A| < |B|$。它们之间不可能存在双射。故 $A \nsim B$。对于无限集合就没有这个性质，前面例 1 中 $N_2 \subset N$，但是 $N_2 \sim N$。

定义 4.19 与自然数集合等势的集合叫做可数无限集合。

有限集合和可数无限集合都称为可数集合。非可数集合称为不可数集合。

若集合 A 与自然数集合 $\mathrm{N} = \{0, 1, 2, \cdots\}$ 等势，那么存在双射 $f: \mathrm{N} \to A$，$f(i) = a_i$，$A = \{a_0, a_1, a_2, \cdots\}$，所以可数无限集合可以逐个地枚举它的元素。自然数集合的势记为$\mathcal{N}_0$。

下面看一个不可数集合的例子。

例 2 $(0, 1) = \{x \mid x \in \mathrm{R}, 0 < x < 1\}$ 是一个不可数集合。这是因为 $C = \left\{\frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{n}, \cdots\right\} \subset (0, 1)$，而 $f: C \to \mathrm{N}$，$f\left(\frac{1}{n}\right) = n - 2$，$f$ 是双射，故 $C \sim \mathrm{N}$，C 是可数无限集合，显然得出 $(0, 1)$ 不是有限集合。

假设 $(0, 1)$是可数无限集合，$(0, 1) = \{b_1, b_2, \cdots, b_n, \cdots\}$，其中

$$b_1 = 0.a_{11}a_{12}\cdots a_{1n}\cdots$$
$$b_2 = 0.a_{21}a_{22}\cdots a_{2n}\cdots$$

$$\cdots$$

$$b_n = 0.a_{1n}a_{2n}\cdots a_{nn}\cdots$$

$$\cdots$$

我们取 $d = 0.d_1d_2\cdots d_n\cdots \in (0, 1)$，其中 $d_i \neq a_{ii}$，0，9，$i = 1, 2, \cdots$。显然 $d_i \neq b_i$，从而 $d \notin \{b_1, b_2, \cdots, b_n, \cdots\} = (0, 1)$，产生矛盾，故 (0，1) 不可能是可数无限集合。从而证明了 (0，1) 是不可数集合。

可以证明 (0，1) 集合与实数集合 R 等势。证明可用图 11 来表示。我们把开区间 (0，1) 的有限长线段弯成一个半圆，用无限长的横坐标轴来表示实数集合 R，横坐标轴与半圆弧相切于圆弧的中点。如果从半圆的圆心引出直线，使之与半圆和横坐标轴相交，这两个交点必然成对出现。从而能够形成从 (0，1) 到 R 的双射。故 (0，1) 与 R 具有相同的势，记作 $\mathscr{N}_1$。

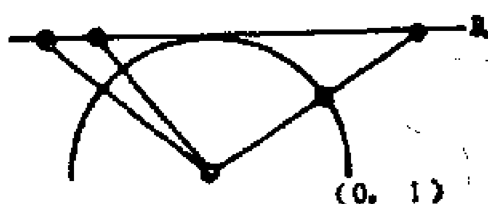


图 11

4.4.2 势的大小

定义 4.20 如果集合 A 与集合 B 的一个子集等势，则称 B 支配 A，记为 $A \precsim B$，并且说 A 的势 $\leqslant B$ 的势。

如果 $A \precsim B$ 且 $A \nsim B$，则称 $A \prec B$，并且说 A 的势 $< B$ 的势。

例如，自然数集合 $N \subset$ 实数集合 R，且 N～N，故自然数集合 N 的势 $\mathscr{N}_0 \leqslant$ 实数集合 R 的势 $\mathscr{N}_1$。又因为 $N \nsim R$，所以 $\mathscr{N}_0 < \mathscr{N}_1$。

定理 4.11 $\mathscr{P}(A)$ 是集合 A 的幂集，那么 A 的势小于 $\mathscr{P}(A)$ 的势，即 $A \prec \mathscr{P}(A)$。

证明 令 $f: A \to \{\{a\} | a \in A\}$，$f(a) = \{a\}$，$f$ 为双射，故 $A \sim \{\{a\} | a \in A\}$。而 $\{\{a\} | a \in A\} \subset \mathscr{P}(A)$，得出 $A \precsim \mathscr{P}(A)$。

假设 $A \sim \mathscr{P}(A)$，则存在双射 $g: A \to \mathscr{P}(A)$。我们把集合 A

的元素分成两类：内部成员和外部成员。如果 $a\in g(A)$，则称 a 为内部成员，否则称为外部成员。令 $B=\{x|x\in A, x\notin g(x)\}\subseteq A$，即 B 是全体外部成员构成的集合，它是 A 的一个子集，$B\in\mathscr{P}(A)$。由于 g 是满射，存在 $b\in A$ 使得 $g(b)=B$。如果这个元素 b 是内部成员，应该 $b\in g(b)=B$，而 B 为外部成员集合，产生矛盾，故不可。如果该 b 是外部成员，应该 $b\notin g(b)=B$，这与 B 是全部外部成员构成的集合相矛盾，故不可。由此得出 $A\not\sim\mathscr{P}(A)$。再联系前面的结论 $A\precsim\mathscr{P}(A)$，得到 $A\prec\mathscr{P}(A)$。**证毕。**

定理 4.12 集合间的支配关系是部分序关系。

证明 对任意集合 A，存在双射 $f:A\to A$，$f(a)=a$。又 $A\subseteq A$，于是 $A\precsim A$。所以支配关系是自反的。如果 $A\precsim B$ 且 $B\precsim C$，即存在双射 $f:A\to B_1$，双射 $g:B\to C_1$，其中 $B_1\subseteq B$，$C_1\subseteq C$。令 $g(B_1)=C_2\subseteq C_1$，g 是从 B_2 到 C_2 的双射，从而 $g\circ f:A\to C_2$ 是双射，而且 $C_2\subseteq C$。于是得出 $A\precsim C$。这就是说支配关系是传递的。

下面证明支配关系的反对称性。已知 $A\precsim B$，$B\precsim A$，即存在双射 $f:A\to B_1$，双射 $g:B\to A_1$，其中 $B_1\subseteq B$，$A_1\subseteq A$，从而 $A\sim B_1$，$B\sim A_1$。令 $g(B_1)=A_2\subseteq A_1\subseteq A$。$g:B_1\to A_2$ 为双射，则 $B_1\sim A_2$。再由等势关系的传递性得出 $A\sim A_2$，即存在双射 $h:A\to A_2$，那么下列式子成立：

$$h(A)=A_2，\text{其中 } A_2\subseteq A_1。\tag{1}$$

$$h(A_1)=A_3，\text{其中 } A_3\subseteq A_2。\tag{2}$$

$$h(A_2)=A_4，\text{其中 } A_4\subseteq A_3。\tag{3}$$

$$h(A_3)=A_5，\text{其中 } A_5\subseteq A_4。\tag{4}$$

……

从而 $A\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_{n-1}\supseteq A_n\cdots$。由(1)和(2)得到 $h(A-A_1)=h(A)-h(A_1)=A_2-A_3$。于是有

$$A-A_1\sim A_2-A_3。\tag{5}$$

由(3)和(4)得到 $h(A_2-A_3)=h(A_2)-h(A_3)=A_4-A_5$。于是有

$$A_2-A_3 \sim A_4-A_5. \tag{6}$$

$$\cdots\cdots.$$

令集合 $C=A_1\cap A_2\cap\cdots\cap A_{n-1}\cap A_n\cap\cdots$，任取集合 A 的元素 a，有如下两种可能性：

1° $a\in A_i$，$i=1, 2, \cdots$，即 $a\in C$。

2° $a\in A_{n-1}-A_n$，$n=1, 2, \cdots$。

显然有

$$A=C\cup(A-A_1)\cup(A_1-A_2)\cup(A_2-A_3)\cup\cdots,$$

$$A_1=C\cup(A_1-A_2)\cup(A_2-A_3)\cup(A_3-A_4)\cup\cdots.$$

又由(5)，(6)，…诸式得到

$$(A-A_1)\cup(A_2-A_3)\cup\cdots\sim(A_2-A_3)\cup(A_4-A_5)\cup\cdots,$$

即存在双射 f_0：$(A-A_1)\cup(A_2-A_3)\cup\cdots\to(A_2-A_3)\cup(A_4-A_5)\cup\cdots$。再定义一个新的映射 $f_1: A\to A_1$，

$$f_1(a)=\begin{cases} f_0(a), & \text{如果 } a\in(A-A_1)\cup(A_2-A_3)\cup\cdots, \\ a, & \text{如果 } a\in C\cup(A_1-A_2)\cup(A_3-A_4)\cup\cdots, \end{cases}$$

不难看出 f_1 是双射，即 $A\sim A_1$。再由 $B\sim A_1$ 推出 $A\sim B$。这就证明了支配关系的反对称性。

综上知支配关系是部分序关系。**证毕。**

4.4.3 无限集合

定理 4.13 每个无限集合都含有一个可数无限子集。

证明 A 是无限集合，显然它不是空集。存在 $a_1\in A$。集合 $A-\{a_1\}$ 仍是无限集合。同理，必存在 $a_2\in A-\{a_1\}$，显然 $a_2\neq a_1$。$\{a_1,a_2\}$ 是 A 的子集。$A-\{a_1, a_2\}$ 也是无限集合。如此进行下去，得到 $S=\{a_1,a_2,\cdots,a_n,\cdots\}$ 是 A 的子集。$i\neq j$，a_i 与 a_j 两两互不相同，那么 S 就是无限集合 A 的可数无限子集。**证毕。**

定理 4.14 每个无限集合都与它自己的一个真子集等势。

证明 A 是无限集合，由定理 4.13 知它有一个可数无限子集 $S=\{a_1, a_2, \cdots, a_n, \cdots\}$。构造映射 $f: A\to A-\{a_1\}$，

$$f(a)=\begin{cases}a, & a\in A-S,\\ a_{i+1}, & a\in S \text{ 且 } a=a_i.\end{cases}$$

f 是双射，即 $A\sim A-\{a_1\}$。**证毕。**

利用本定理，定义 4.18 可以改写成：一个集合如果与其真子集等势，就称这个集合为无限集合，不是无限集合的称为有限集合。

习　题

1. E 是万有集合. 在 $\mathscr{P}(E)$ 上定义的下列关系具有什么性质？

(1) $S\rho_1T \Leftrightarrow S\cap T=\varnothing$.

(2) $S\rho_2T \Leftrightarrow S\cap T\neq\varnothing$.

(3) $S\rho_3T \Leftrightarrow S\subset T$.

(4) $S\rho_4T \Leftrightarrow S\subseteq T$.

(5) $S\rho_5T \Leftrightarrow S=T$.

2. 在整数集合 Z 上给出三个关系，它们分别具有如下性质：

(1) 自反、对称，但不是传递的.

(2) 自反，传递，但不是对称的.

(3) 对称，传递，但不是自反的.

3. 令 $A=\{a,b,c,d\}$，R_1 和 R_2 是 A 上的关系，其中

$$R_1=\{(a,a),(a,b),(b,d)\},$$

$$R_2=\{(a,d),(b,c),(b,d),(c,b)\},$$

求 $R_1\circ R_2$，$R_2\circ R_1$，R_1^2，R_2^3。

4. R_1 是从集合 B 到集合 C 的关系，R_2 和 R_3 是从集合 A 到集合 B 的关系. 证明：

$$R_1\circ(R_2\cap R_3)\subseteq R_1\circ R_2\cap R_1\circ R_3.$$

5. 证明 $R'=I_A\cup R$ 是 R 的自反闭包.

6. N 是自然数集合，$\sim$ 是 N×N 上的关系，(a,b)，$(c,d)\in$ N×N。

$$(a,b)\sim(c,d) \Leftrightarrow a+d=b+c.$$

证明 $\sim$ 是 N×N 上的等价关系，并在 $x-y$ 平面上画出 $\sim$ 所确定的等价类.

7. 令 $A=\{1,2,3,4\}$. 在 $\mathscr{P}(A)$ 中定义关系 $\sim$：

$$S\sim T \Leftrightarrow |S|=|T|.$$

证明 $\sim$ 是 $\mathscr{P}(A)$ 上的等价关系，并写出它的商集 $\mathscr{P}(A)/\sim$。

8. R^* 为非零实数集合，$x,y\in R^*$，定义 R^* 上的关系 ρ

$$x\rho y \Leftrightarrow x\cdot y>0.$$

证明：ρ 是 R^* 上的等价关系，列出所有等价类的代表元。

9．R 为实数集合，在 R 上定义关系 ρ，$x,y\in \mathrm{R}$，

$$x\rho y \Leftrightarrow x \text{ 与 } y \text{ 相差一个整数}.$$

证明：ρ 是 R 上的等价关系．写出全部等价类的代表元．

10．R 是集合 X 上的部分序．A 是 X 的子集，证明 $R\cap(A\times A)$ 是 A 上的一个部分序．

11．A 是非空集合．集合 A 上的全体二元关系组成集合 B．R_1，$R_2\in B$．如果 x，$y\in A$，且 xR_1y 则必有 xR_2y．那么记 $R_1\leqslant R_2$．证明 $\langle B,\leqslant\rangle$ 是部分序集．

12．画出下列集合上整除关系的 Hasse 图．

(1) $\{1,2,3,4,6,8,12,24\}$．

(2) $\{1,2,3,4,5,6,7,8,9,10,11,12\}$．

13．画出图 12 中各关系的 Hasse 图．

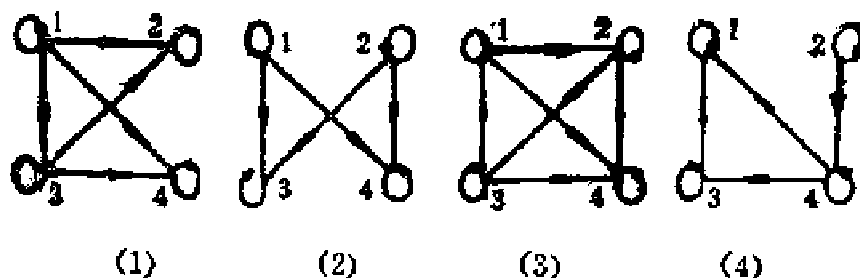


图 12

14．说明只包含三个元素的部分序集共有五种不同的 Hasse 图．

15．Z 为整数集合，在 $\mathrm{Z}^*=\mathrm{Z}-\{0\}$ 上定义 $\leqslant$ 关系，$m,n\in \mathrm{Z}^*$．

$$m\leqslant n \Leftrightarrow m\cdot n>0 \text{ 且 } m|n.$$

证明：$\langle \mathrm{Z}^*,\leqslant\rangle$ 是部分序集．它是否有最大元，最小元，极大元，极小元？

16．A 是任意集合，在部分序集 $\langle \mathscr{P}(A),\subseteq\rangle$ 中取子集序列 $\{a_1\}$，$\{a_1,a_2\}$，$\{a_1,a_2,a_3\}$，…，$\{a_1,a_2,\cdots,a_n\}$，…，它们的并集是否是 $\mathscr{P}(A)$ 的一个极大元？为什么？

17．$\langle S,\leqslant\rangle$ 是部分序集．S 的任一非空子集 M 均含有极小元当且仅当 S 的递降序列 $a_1>a_2>\cdots>a_n>\cdots$ 必终止于有限项．

18．证明一个有限集合与一个可数集合的并是可数集合．

19．证明 $\mathrm{N}\times\mathrm{N}$ 是可数集合，这里 N 是自然数集合．

20．证明 $\mathrm{R}\times\mathrm{R}$ 与实数集合 R 等势．

5 群论初步

从本章起开始讲述群，环，域，格等代数对象的基本性质。它是学习和研究理论计算机科学不可缺少的工具。

今后我们主要研究对象不是代数结构中的元素特性，而是各种代数结构本身和不同代数结构之间的相互联系(同态)。掌握其中体现的丰富的数学思想和方法，比背诵定义和名词要重要得多。

5.1 群的定义与简单性质

定义 5.1 G **是非空集合，** $*$ **是** G **上的乘法运算，如果它们满足如下要求：**

1° G **对于乘法** $*$ **是封闭的，即** $\forall a, b \in G$, $a*b \in G$。

2° $\forall a, b, c \in G$ $a*(b*c) = (a*b)*c$。$*$ **满足结合律。**

3° **存在** $e \in G$, $\forall a \in G$ $e*a = a*e = a$。 e **称为单位元。**

4° $\forall a \in G$, **存在** $a' \in G$ **使得** $a'*a = a*a' = e$。a' **称为** a **的逆元。**

那么 G **连同** $*$ **称为一个群，记为** $\langle G, *\rangle$。

如果只满足 1°, 2°，则称 $\langle G, *\rangle$ 为半群。

如果只满足 1°, 2°, 3°，则称 $\langle G, *\rangle$ 为带 1 半群。

定义 5.2 在群 $\langle G, *\rangle$ **中，如果对任意** $a, b \in G$, $a*b = b*a$，**则称** $\langle G, *\rangle$ **为交换群(或称为阿贝尔群)。**

例 1 A 是非空集合。$\langle \mathscr{P}(A), \cup \rangle$ 是带 1 半群。$\varnothing \in \mathscr{P}(A)$ 是单位元。

例 2 字母表 Σ 上的所有非空字组成集合 Σ^+，对于字的连接

运算·构成半群$\langle \Sigma^+, \cdot \rangle$

例 3 有理数集合Q，在普通加法运算之下形成交换群，$\langle Q, +\rangle$。其单位元为0，每个元素的逆元就是它的负数。

例 4 非零实数集合R^*，在普通乘法运算之下形成交换群。$\langle R^*, \cdot\rangle$。其单位元为1。每个元素的逆元就是它的倒数。

例 5 令$G=\{1, -1, i, -i\}$，对于复数乘法构成有限交换群$\langle G, *\rangle$。G中任意两个元素的乘积可用下面的群表表示

*	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

例 6 令$Z_n=\{[0],[1],\cdots,[n-1]\}$，其中$[i]$是模$n$同余$i$的所有整数构成的集合。我们在$Z_n$中规定+运算，$[a]+[b]=[a+b]$。由模$n$同余类定义知，如果$[a_1]=[a_2]$，$[b_1]=[b_2]$，那么$[a_1+b_1]=[a_2+b_2]$，即同余类的加法定义与同余类的代表元选取是无关的。所以这样的加法定义是确定的，我们称它是“可定义”的。不难验证$\langle Z_n, +\rangle$是交换群，$[0]$是它的单位元，$[a]$的逆元是$[-a]$。

从群的定义，我们可以定义群G中元素的方幂

$$a^n=\overbrace{a*a*\cdots*a}^{n}.$$

显然$a^m*a^n=a^{m+n}$，$(a^m)^n=a^{m\cdot n}$。如果将G中元素a的逆元a'记成a^{-1}，那么

$$a*a'=a*a^{-1}=a^0,$$

即$a^0=e$。 显然$a^{-n}=(a^{-1})^n=(a')^n$。

在群$\langle G, *\rangle$中的运算$*$不一定满足交换律。当运算$*$满足交换律时，一般写作“+”。群的单位元称为零元。元素的逆元称为负元。在交换群中，

$$na = \overbrace{a + a + \cdots + a}^{n},$$

$$ma + na = (m+n)a,$$

$$m(na) = (m \cdot n)a.$$

定理 5.1　在群 $\langle G,*\rangle$ 中左消去律和右消去律成立，即 $\forall\, a, b \in G$，如果 $a*b = a*c$，则必有 $b = c$。如果 $b*a = c*a$，则必有 $b = c$。

证明　如果 $a*b = a*c$，由群定义中 4°知，G 中每个元素都有逆元。元素 a 的逆元为 a'。我们用 a' 左乘这个等式

$$a'*(a*b) = a'*(a*c),$$

又由群定义中的2°知，运算 $*$ 满足结合律，得到 $(a'*a)*b = (a'*a)*c$。从逆元的定义和单位元 e 的定义知 $a'*a = e$，$e*b = b$，$e*c = c$，于是最后得到 $b = c$。这表明在群 G 的等式中可以消去等式两边最左的公因子，即左消去律成立。

同理可以证明右消去律成立。**证毕。**

定理 5.2　在群 $\langle G,*\rangle$ 中，方程 $a*x = b$ 与 $y*a = b$ 有唯一解。

证明　令 $x = a'*b$ 代入方程 $a*x = b$ 中，使得

$$a*(a'*b) = (a*a')*b = e*b = b,$$

它说明 $x = a'*b$ 是方程 $a*x = b$ 的解。

现假设 x_1 和 x_2 都是方程 $a*x = b$ 的解，即 $a*x_1 = b$，$a*x_2 = b$。于是有 $a*x_1 = a*x_2$，利用左消去律得到。$x_1 = x_2$。这就是说如果方程 $a*x = b$ 有两个解，那么它们必需相等。

综上知在群 $\langle G,*\rangle$ 中方程 $a*x = b$ 有解，并且解是唯一的。

同理可以证明方程 $y*a = b$ 有唯一解。**证毕。**

定理 5.3　群 $\langle G,*\rangle$ 中单位元和逆元是唯一的。

证明　假设 e_1 和 e_2 都是群 G 的单位元。因为 e_1 是单位元，$\forall a \in G$　$a*e_1 = a$，特别取 $a = e_2$，那么 $e_2*e_1 = e_1$。又因 e_2 是单位元，$\forall a \in G$，$e_2*a = a$，特别取 $a = e_1$，那么 $e_2*e_1 = e_2$。从而 $e_1 = e_2$，即群 G 的单位元是唯一的。

假设 $a_1, a_2 \in G$ 都是 a 的逆元。由逆元定义知 $a_1 * a = e$，$a_2 * a = e$，即 $a_1 * a = a_2 * a$。再用右消去律得到 $a_1 = a_2$，即是群 G 中元素 a 的逆元是唯一的。**证毕。**

定理 5.4　在群 $\langle G, * \rangle$ 中，$\forall a, b \in G$。

1°　$(a')' = a$。

2°　$(a*b)' = b' * a'$。

证明

1°　$(a')'$ 是 a' 的逆元，a' 是 a 的逆元，由逆元的定义知 $(a')' * a' = e$，$a * a' = e$，即 $(a')' * a' = a * a'$。由右消去律知 $(a')' = a$。

2°

$$(a*b)*(b'*a') = a*(b*b')*a' = a*a' = e,$$
$$(b'*a')*(a*b) = b'*(a'*a)*b = b'*b = e.$$

由逆元的唯一性知 $(a*b)' = b'*a'$。**证毕。**

注意，在群中乘积求逆满足脱衣规则。

定义 5.3　在群 $\langle G, * \rangle$ 中，G 是有限集合，则称 $\langle G, * \rangle$ 是有限群，其阶数为 $|G|$。

定义 5.4　在群 $\langle G, * \rangle$ 中，$a \in G$，如果存在 n，它是满足 $a^n = e$ 的最小正整数，则称元素 a 是 n 阶的。如果那样的 n 不存在，则称元素 a 是无限阶的。

我们考虑集合 A，其中 $a \in G$，Z^* 为非零整数集合，

$$A = \{i \mid i \in Z^*, a^i = e\}$$

当 $A = \varnothing$ 时，a 是无限阶元。当 $A \neq \varnothing$ 时，那么 A 中必有正整数。(这是因为如果 $-m < 0$，且 $-m \in A$ 即 $a^{-m} = e$，那么必有 $a^m = e$，即 $m > 0$ 且 $m \in A$。) 这时 a 是有限阶的，其阶数是 A 中的最小正整数 n。集合 A 有如下性质

1°　若 $m, l \in A$，则 $m \pm l \in A$。

2°　若 $m \in A$，$c \in Z^*$，则 $cm \in A$。

不难证明

$$A = \{kn \mid k \in Z^*\}.$$

也就是说，如果 $a^m=e$，那么 m 必是元素 a 阶的整数倍数。

例 1 在整数加群 $\langle Z,+\rangle$ 中，除零元 0 的阶为 1 以外，所有元素的阶都是无限的。

例 2 模 6 同余类群 $\langle Z_6,+\rangle$ 中，[0]是 1 阶元，[1]，[5]是 6 阶元，[2]，[4] 是 3 阶元，[3] 是 2 阶元。

例 3 在群 $\langle G,*\rangle$ 中，$a,b\in G$，它们分别是 m 阶、n 阶元，$(m,n)=1$。如果 $a*b=b*a$，则 $a*b$ 是 $m\cdot n$ 阶元。

证明 设 $a*b$ 的阶为 k，

$$(a*b)^{mn}=a^{mn}*b^{mn}=(a^m)^n*(b^n)^m=e*e=e,$$

得知 $k|mn$。

由于 $a*b$ 的阶是 k，$(a*b)^k=e$，

$$e=(a*b)^{km}=(a^m)^k*b^{km}=b^{km}.$$

因为 b 的阶为 n，故 $n|km$，又由 $(m,n)=1$ 知 $n|k$。同理可以证明 $m|k$。从而 $[m,n]|k$，即 $mn|k$。

综上知 $k=m\cdot n$。

5.2 群定义的进一步讨论

本节介绍群的几个等价的定义.从而更进一步探讨群的性质.

定理 5.5 *G* **是非空集合，*** **是** *G* **上的运算．如果**

(1) $\forall a,b\in G$，$a*b\in G$，

(2) $\forall a,b,c\in G$，$a*(b*c)=(a*b)*c$，

(3) **存在** $e_r\in G_1$，**对一切** $a\in G$，$a*e_r=a$。e_r **称为右单位元，**

(4) $\forall a\in G$，**存在** $a'\in G$ **使得** $a*a'=e_r$。a' **称为** a **的右逆，**

那么 $\langle G,*\rangle$ 为群。

证明 对照定义 5.1，我们只要证明右单位元一定是左单位元，右逆一定是左逆。

先证右逆一定是左逆，即已知 $a*a'=e_r$，证明 $a'*a=e_r$。现设 a'' 是 a' 的右逆，$a'*a''=e_r$。

$$a'*a=(a'*a)*e_r=(a'*a)*(a'*a'')=a'*a''=e_r.$$

a'也是 a 的左逆。

再证右单位元一定是左单位元。a' 是 a 的逆元

$$e_r*a=(a*a')*a=a*(a'*a)=a*e_r=a$$

证毕。

定理 5.6 G **是非空集合，**$*$ **是** G **上的运算，如果**

1) $\forall a,b\in G$，$a*b\in G$。

2) $\forall a,b,c\in G$，$(a*b)*c=a*(b*c)$。

3) $\forall a,b\in G$，**方程** $a*x=b$ **和** $y*a=b$ **在** G **中都有解。**

那么 $\langle G,*\rangle$ **为群。**

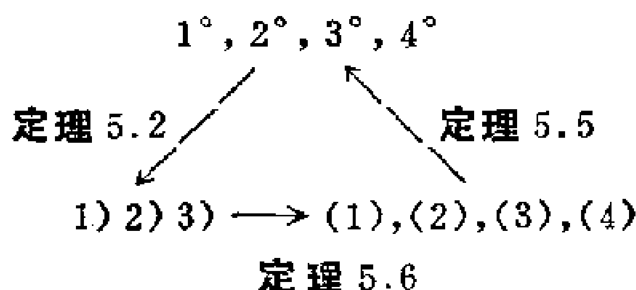
证明 与定理 5.5 比较，我们要证明从(3)推出 G 中有右单位元并且任意元素均有右逆。

由 3) 知方程 $a*x=a$ 在 G 中有解，我们选取其中一个记为 e_r，即 $a*e_r=a$。任取 G 的任意元素b，由 3) 知 $y*a=b$ 在 G 中有解，我们选取其中一个记为 d，即 $d*a=b$。那么

$$b*e_r=(d*a)*e_r=d*(a*e_r)=d*a=b.$$

这说明 e_r 是 G 的右单位元。又由 3) 知 $a*x=e_r$ 在 G 中有解，并记为 a'，即 $a*a'=e_r$，那么 a' 是 a 的右逆。**证毕。**

定理 5.5 和定理 5.6 是与定义 5.1 等价的两个群定义。它们的等价性证明过程如下图所示。



定理 5.7 G **是有限集合，**$*$ **是** G **上的运算。如果**

1° $\forall a,\ b\in G$，$a*b\in G$，

2° $\forall a,b,c\in G$，$(a*b)*c=a*(b*c)$，

3° $\forall a\in G$ $a*x_1=a*x_2$ **推出** $x_1=x_2$，**或者**$\forall a\in G$，$y_1*a=y_2*a$

推出 $y_1=y_2$，

那么 $\langle G,*\rangle$ **是群。**

证明 令 $G=\{a_1, a_2, \cdots, a_n\}$。任取 G 中的元素 a，用 a 左乘 G 的每个元素，所有乘积构成一个集合 G'

$$G'=\{a*a_1, a*a_2, \cdots, a*a_n\}.$$

由 $1°$ 知 $a*a_i\in G$，$1\leqslant i\leqslant n$，即 $G'\subseteq G$。又由 $3°$ 知当 $i\neq j$ 时，$a*a_i\neq a*a_j$，于是 $|G'|=|G|=n$。显然得出 $G=G'$。这表明任取 G 的元素 a,b，方程 $a*x=b$ 均有解。

同样，考虑 $G''=\{a_1*a, a_2*a, \cdots, a_n*a\}$，可以证明任取 G 的元素 a,b，方程 $y*a=b$ 均有解。

由定理 5.6 知 $\langle G,*\rangle$ 为群。**证毕。**

在定理 5.1 中指出，在群中左、右消去律成立。现在定理5.7 中，如果非空集合 G 上的运算满足封闭性，结合律和左右消去律，那么该代数结构是群。也就是说，当 G 是有限集合时，定义 5.1 的 $1°$，$2°$，$3°$，$4°$，与定理 5.7 中的 $1°$，$2°$，$3°$ 是等价的。从而定理 5.7 可以看成有限群的定义。

一个有限群的乘法可以用一个群来表示。群的一些性质可以从这个表上直接看出：由于存在单位元，表中有一行与横线上边的元素一样，表里有一列与竖线左边的元素一样。又由消去律知，全体元素必在每行出现一次，必在每列出现一次。下面我们来看几个低阶群。

一阶群 G_1，$|G_1|=1$。由于群必有单位元 e，所以 $G_1=\{e\}$。二阶群 G_2，$|G_2|=2$。G_2 中除去单位元之外还有一个元素 a。$G_2=\{e, a\}$，$a\neq e$。由运算 $*$ 的封闭性，$a*a\in\{e,a\}$。假设 $a*a=a$。由 $a*e=a$ 推出 $a=e$，矛盾，故不可。所以 $a*a=e$。G_1 与 G_2 的乘法表如下：

*	e
e	e

G_1

*	e	a
e	e	a
a	a	e

G_2

三阶群 $G_3=\{e,a,b\}$，$a\neq b$，$a,b\neq e$。$a*a$ 不能是 a 或 e，否则推出 $a=e$，所以 $a*a=b$。再根据每个元素在一行或一列中出现且只出现一次，得到 $a*b=e$，$b*a=e$，$b*b=a$。我们看到元素 $b=a*a=a^2$，$e=b*a=a^3$，从而 $G_3=\{e,a,a^2\}$，并且 a 是三阶元，$a^3=e$。四阶群在同构的意义下只有两个：$C_4=\{e,a,a^2,a^3\}$ 且 $a^4=e$，$K_4=\{e,a,b,c\}$ 且 $a^2=b^2=c^2=e$。三阶群 G_3 和四阶群 C_4，K_4 的乘法表如下：

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

G_3

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

C_4

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

K_4

例 1 若 G 是有限群，则 G 的每个元素的阶，必是有限的。

证明 群 G 的单位元 e 显然是 1 阶元。若 $a\in G$ 且 $a\neq e$，$a,a^2,a^3,\cdots,a^n,\cdots\in G$。由于 G 是有限集合，必然存在 $i>j$，$a^i=a^j$。等式两边同时乘以 a^j 的逆元 $(a^j)'$，

$$a^i*(a^j)'=a^j*(a^j)'=e.$$

由 $a^i=a^{i-j}*a^j$，及 $*$ 运算的结合律得到

$$a^{i-j}=e,\ i-j>0.$$

那么 $i-j$ 是上节末提到的集合 $A=\{k|k\in Z^*,\ a^k=e\}$ 的元素 $A\neq\varnothing$，这表明元素 a 是有限阶元，其阶数是 A 中的最小正整数。**证毕**。

下面再给出两个非交换群的例子。

例 2 全体 n 阶有理数方阵记为Q_n。令 $G=\{A|A\in Q_n,|A|\neq 0\}$。$G$ 对于矩阵乘法 $\cdot$ 构成群。若 $A,B\in G$，即 $|A|,|B|\neq 0$，而 $|A\cdot B|=|A|\cdot|B|\neq 0$，则 $A\cdot B\in G$。乘法 $\cdot$ 在 G 中是封闭的。矩阵乘法是可结合的。

$$I_n=\begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}$$

是 G 的单位元。当 $A\in G$ 时，$|A|\neq 0$，A 有逆矩阵 A^{-1}，且 $|A^{-1}|\neq 0$，即 $A^{-1}\in G$，且 $A\cdot A^{-1}=I_n$，故 A^{-1} 是 A 在 G 中的逆元。所以 $\langle G,\cdot\rangle$ 为群。由于矩阵乘法是非交换的，于是 $\langle G,\cdot\rangle$ 为非交换群。

例 3 Q是有理数集合。令

$$G=\{f_{a,b}\mid f_{a,b}:\mathrm{Q}\to\mathrm{Q},f_{a,b}(x)=ax+b,a\neq 0,a,b\in\mathrm{Q}\}.$$

G 对于映射的合成运算。构成群。若 $f_{a,b},f_{c,d}\in G$，其中 $f_{a,b}(x)=ax+b$，$f_{c,d}(x)=cx+d$，且 $a,c\neq 0$，$a,b,c,d\in\mathrm{Q}$，

$$(f_{a,b}\circ f_{c,d})(x)=f_{a,b}(cx+d)=a(cx+d)+b=f_{ac,ad+b}(x),$$

其中 $a\cdot c\neq 0,ac,ad+b\in\mathrm{Q}$，故 $f_{a,b}\circ f_{c,d}\in G$，即 G 中 $\circ$ 运算是封闭的。映射合成运算是可结合的。$f_{1,0}\in G$ 是 G 的单位元。$f_{\frac{1}{a},-\frac{b}{a}}$ 是 $f_{a,b}$ 的逆元，$\langle G,\circ\rangle$ 是群。由于运算 $\circ$ 不满足交换律，所以 $\langle G,\circ\rangle$ 是非交换群。

5.3 子　　群

定义 5.5 **$\langle G,*\rangle$ 是群，H 是 G 的非空子集。如果**

1° $\forall a,b\in H$，$a*b\in H$，

2° $\forall a\in H$，$a'\in H$，

则称 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的子群，并记为 $H\leqslant G$。

定理 5.8 **若 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的子群，则 $\langle H,*\rangle$ 也是群。**

证明 从 $\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的子群定义知运算 $*$ 在集合 H 中是封闭的。H 是 G 的子集。即 H 中的每个元素都是 G 中的元素，而 $\langle G,*\rangle$ 是群。$*$ 运算满足结合律，从而 $\forall a,b,c\in H\subseteq G$，$(a*b)*c=a*(b*c)$。$H$ 是 G 的非空子集，它至少有一个元素 $h\in H$，由子群定义中 2° 知 $h'\in H$，那么 $h*h'=e\in H$。故 G 中的单位元 e 在 H 中并且也是 H 的单位元。综上知 $\langle H,*\rangle$ 本身也是群。**证毕。**

由此看出，群 G 的子集，如果对该群的运算及求逆运算是封

闭的，那么该子集对原来群的运算也构成群。

定理 5.9 **H 是群 G 的有限非空子集。如果 $\forall a, b\in H, a*b\in H$，则 $H\leqslant G$。**

证明 任取 $a\in H$，$a^2=a*a\in H$，$a^3=a^2*a\in H$，…。由于 H 是 G 的有限非空子集，$a, a^2, a^3, \cdots$ 不可能是完全不同的元素，必存在 $1\leqslant i<j$，使得 $a^i=a^j=a^i*a^{j-i}$。用左消去律得到 $a^{j-i}=e\in H$。

$$e=a^{j-i}=a*a^{j-i-1},\quad j-i-1\geqslant 0.$$

$a'=a^{j-i-1}\in H$，这表明 H 中的任意元素 a 在 H 中均有逆。对照定义 5.5 知 $\langle H, *\rangle$ 是 $\langle G, *\rangle$ 的子群。**证毕**

例 1 $\langle G, \cdot\rangle=\langle\{1, -1, i, -i\}, \cdot\rangle$ 中，$H=\{1, -1\}\subset G$。H 对复数乘法运算封闭，$\langle H, \cdot\rangle$ 是 $\langle G, \cdot\rangle$ 的子群。

例 2 全体非零复数集合 C^*，对复数乘法构成群 $\langle C^*, \cdot\rangle$。令

$$H=\{x \mid x\in C^*, \exists n\in N \text{ 使 } x^n=1\},$$

则 $H\leqslant C^*$。

证明 1 是群 $\langle C^*, \cdot\rangle$ 的单位元。$1^1=1$，$1\in H$。H 是 C^* 的非空子集。若 $x, y\in H$，即存在 $n, m\in N$，使 $x^n=y^m=1$，而 $(x\cdot y)^{mn}=(x^n)^m\cdot(y^m)^n=1$，故 $x\cdot y\in H$。又若 $x\in H$，存在 $n\in N$，$x^n=1$。而 $(x')^n=(x^n)'=1'=1$，故 $x'\in H$。这就证明了 $H\leqslant C^*$。

例 3 设 $H_1\subseteq H_2\subseteq\cdots\subseteq H_n\subseteq\cdots$ 是由群 G 的子群 H_i 组成的升链。令 $H=\bigcup_i H_i$，则 $H\leqslant G$。

证明 H_i 是群 G 的子群。即 $H_i\neq\varnothing$ 且 $H_i\subseteq G$，显然 $H=\bigcup_i H_i\neq\varnothing$ 且 $H\subseteq G$。若 $a, b\in H$，存在 $i, j, i>j$ 使 $a\in H_i$，$b\in H_j\subseteq H_i$，由于 $H_i\leqslant G$，则 $a*b\in H_i\subseteq H$。又若 $a\in H$，存在 i，$a\in H_i$。再由 $H_i\leqslant G$，则 $a'\in H_i\subseteq H$。综上知 $H\leqslant G$。

例 4 $\langle G, *\rangle$ 是群。S 是 G 的非空子集。令

$$A=\{H \mid H\leqslant G \text{ 且 } S\subseteq H\},$$

即 A 是 G 中包含 S 的所有子群构成的集合。显然 $G\in A$，即 A

是非空的．定义 $K=\bigcap\limits_{H\in A}H$。证明$K\leqslant G$。

证明 任取 $H\in A$，H 是 G 的子群。群 G 的单位元 $e\in H$ 且 $H\subseteq G$，所以 $e\in\bigcap\limits_{H\in A}H=K$ 且 $K\subseteq G$，即 K 是 G 的非空子集。若 a，$b\in K$，对任何 $H\in A$ 均有 a，$b\in H$，H 是 G 的子群，故 $a*b\in H$。所以 $a*b\in K$，又若$a\in K$，对任何 $H\in A$ 均有 $a\in H$，H 是 G 的子群，故 $a'\in H$。所以 $a'\in K$，综上知 $K\leqslant G$。

A 中的每个 H 均满足 $S\subseteq H$。显然 $S\subseteq\bigcap\limits_{H\in A}H=K$。从而 K 是 G 中包含 S 的最小子群。我们记 $\langle S\rangle=K=\bigcap\limits_{H\in A}H$，并称 $\langle S\rangle$为 S 生成的子群。如果 S 本身就是 G 的子群，那么 $K=\langle S\rangle=S$，否则 $S\subsetneq\langle S\rangle$。

下面讨论 $\langle S\rangle$ 是由哪些元素组成的。我们先引入集合T。

$$T=\{a_1^{e_1}*a_2^{e_2}*\cdots*a_n^{e_n}\mid a_1,a_2,\cdots,a_n\in S,e_1,e_2,\cdots,e_n=\pm1,\\ n=1,2,\cdots\}.$$

S是非空集合。S中的任意元素a，$a=a^1$，故 $a\in T$，也就是说$S\subseteq T$，T是非空集合。由T的定义知$T\subseteq G$。若 $x=a_{t_1}^{e_{t_1}}*a_{t_2}^{e_{t_2}}*\cdots*a_{t_m}^{e_{t_m}}$，$y=a_{j_1}^{e_{j_1}}*a_{j_2}^{e_{j_2}}*\cdots*a_{j_n}^{e_{j_n}}\in T$，那么 $x*y=a_{t_1}^{e_{t_1}}*\cdots a_{t_m}^{e_{t_m}}*a_{j_1}^{e_{j_1}}*\cdots*a_{j_n}^{e_{j_n}}\in T$，$x'=a_{t_1}^{-e_{t_1}}*a_{t_2}^{-e_{t_2}}*\cdots*a_{t_m}^{-e_{t_m}}\in T$，所以$T$是 G 的包含 S 的子群。前面已经知道 $\langle S\rangle$ 是 G 中包含 S 的最小子群，于是 $\langle S\rangle\subseteq T$。

另一方面，任取 $x=a_{t_1}^{e_{t_1}}*a_{t_2}^{e_{t_2}}*\cdots*a_{t_m}^{e_{t_m}}\in T$，其中 $a_{t_k}\in S$，$e_{t_k}=\pm1$，$1\leqslant k\leqslant m$。由于 $\langle S\rangle$ 是包含 S 的群，$a_{t_k}^{e_{t_k}}\in\langle S\rangle$，$1\leqslant k\leqslant m$，所以 $x\in\langle S\rangle$。由此推出 $T\subseteq\langle S\rangle$。

综上知 $T=\langle S\rangle$。

特别地，当 $S=\{a\}$ 时，$\langle S\rangle=\{a^n\mid n\in Z\}=\langle a\rangle$。整数加群 $\langle Z,+\rangle$ 是由整数 1 生成的群，即 $\langle Z,+\rangle=\langle 1\rangle$。$\langle 2\rangle=\{2k\mid k\in Z\}$，$\langle 2,3\rangle=\{2a+3b\mid a,b\in Z\}=\{k\cdot 1\mid k\in Z\}=Z$。一般地 $\langle m,n\rangle=\{(m,n)\cdot k\mid k\in Z\}$。

5.4 循 环 群

有一类群，它的每个元素都可以写成某个固定元素的幂，a^i或a^{-i}，这样的群称之为循环群。

定义 5.6 在群 $\langle G, *\rangle$ 中，如果存在一个元素 $g \in G$，使 $G=\{g^n \mid n \in Z\}$，则称该群为循环群，记作$\langle g\rangle$，其中 g 称为循环群的生成元。

若群中的运算用"+"表示，循环群 $\langle G, +\rangle$ 写成$\langle g\rangle=\{ng \mid n \in Z\}$，$g$ 是该循环群的生成元。

每个循环群都是交换群，这是因为$g^r * g^s = g^{r+s} = g^s * g^r$。

例 1 $\langle G, *\rangle = \langle\{1, -1, i, -i\}, \cdot\rangle$ 是由 i 生成的四阶循环群。

$$i^0=1,\ i^1=i,\ i^2=-1,\ i^3=-i,\ i^4=1,\ \cdots$$

所以该群可以写成 $\langle\{1, i, i^2, i^3\}, \cdot\rangle$。

定理 5.10 g 是群$\langle G, *\rangle$中 k 的阶元．令 $H=\{g^r \mid r \in Z\}$，那么 $\langle H, *\rangle$ 是 $\langle G, *\rangle$ 的一个 k 阶子群。

证明 $\forall r, s \in Z$，$g^r * g^s = g^{r+s} \in H$，$(g^r)' = g^{-r} \in H$．故 $H \leqslant G$．g 是 G 的 k 阶元，$g^0=e, g^1, \cdots, g^{k-1}$ 是 k 个两两互不相同的元素。对于任意整数 t，$t=uk+v$，其中 $0 \leqslant v < k$，那么

$$g^t = g^{uk+v} = (g^k)^u * g^v = g^v$$

$$H=\{g^r \mid r \in Z\}=\{g^0, g^1, \cdots, g^{k-1}\}.$$

$\langle H, *\rangle$ 是 $\langle G, *\rangle$ 的 k 阶子群。

特别地，G 是 n 阶群。G 的某个元素 g 是 n 阶元，那么 G 必定是由 g 生成的一个循环群。

定理 5.11 循环群的每个子群必是循环群。

证明 令 G 是由元素 a 生成的循环群。$G=\langle a\rangle$。H 是群 G 的子群。如果 $H=\{e\}=\langle e\rangle$，显然 H 是循环群．如果 $H \neq \{e\}$。那么至少存在一个元素 $b \in H$ 且 $b \neq e$。由于 H 是 G 的子集，

$G=\langle a\rangle$，那么必然存在 l（不妨假设 l 为正整数），使 $b=a^l$。设 m 是使 $a^m\in H$ 的最小正整数，任取 H 中的元素 b，b 也是群 G 的元素，故 $b=a^n$。令 $n=mu+v$，$0\leqslant v<m$，

$$b=a^n=a^{mu+v}=(a^m)^u * a^v,$$

$$a^v=a^n*(a^m)^{-u}.$$

由于 $b=a^n\in H$，$a^m\in H$，而 H 是群，$(a^m)^{-u}\in H$，从而 $a^v\in H$。假若 $v>0$，那么这就与 m 是使 $a^m\in H$ 的最小正整数相矛盾，故不可。这说明必需 $v=0$，即 $b=a^{mu}=(a^m)^u$，也就是说 H 中的每个元素都可以表示成 a^m 的方幂。于是 a^m 是子群 H 的生成元。H 是循环群。

例 2 模 6 同余类加群 $\langle Z_6,+\rangle=\langle[1]\rangle$ 是循环群。[0] 是 1 阶元，$\langle[0]\rangle=\{[0]\}$ 是 Z_6 的 1 阶子群 [3] 是 2 阶元，$\langle[3]=\{[0],[3]\}$ 是 Z_6 的 2 阶子群。[5]是 6 阶元，$\langle[5]\rangle=\{[0],[5],[4],[3],[2],[1]\}$ 是 Z_6 的 6 阶子群。

定理 5.12 G **是** n **阶循环群，**$G=\langle a\rangle$ **且** $|G|=n$。H **是** G **的一个子群，**$H=\langle b\rangle$，**且** $b=a^s$，**则**

$$|H|=\frac{n}{(n,s)}.$$

证明 令 H 是 G 的 m 阶子群，m 是使 $b^m=e$ 的最小正整数。$b^m=a^{sm}=e$，而 a 是 n 阶元 $a^n=e$，故 $n|ms$。设 $(n,s)=d$，$n=dn_0$，$s=ds_0$，且 $(n_0,s_0)=1$，于是 $n_0|ms_0$，进而得到 $n_0|m$，即 $m=n_0\cdot k$。m 是满足此式的最小正整数，从而 $k=1$。最后得出

$$m=n_0=\frac{n}{(n,s)}.$$

证毕。

例 3 求模 18 同余类加群的所有子群。

解 $\langle[1]\rangle=\langle[5]\rangle=\langle[7]\rangle=\langle[11]\rangle=\langle[13]\rangle=\langle[17]\rangle$ 是 Z_{18} 的 18 阶子群。

$\langle[2]\rangle=\langle[4]\rangle=\langle[8]\rangle=\langle[10]\rangle=\langle[14]\rangle=\langle[16]\rangle$ 是 Z_{18} 的

9 阶子群。

$\langle[3]\rangle=\langle[15]\rangle$ 是 Z_{18} 的 6 阶子群。

$\langle[6]\rangle=\langle[12]\rangle$ 是 Z_{18} 的 3 阶子群。

$\langle[9]\rangle$ 和 $\langle[0]\rangle$ 分别为 Z_{18} 的 2 阶和 1 阶子群。

例 4 在集合 $\{1,2,\cdots,p-1\}$ 上定义运算 $*$：

$$a*b=c \Longleftrightarrow a\cdot b\equiv c \pmod p,$$

其中 p 为素数。若 $a\in\{1,2,\cdots,p-1\}$，显然 $(a,p)=1$，a 的阶为 l，那么 $l\mid(p-1)$，即 a 是 $x^l\equiv1\ (\mathrm{mod}\,p)$ 的一个解。于是 $\{1,a,a^2,\cdots,a^{l-1}\}$ 都是 $x^l\equiv1(\mathrm{mod}\,p)$ 的解，而且是全部解。它是以 a 为生成元的 l 阶循环群，是 $\{1,2,\cdots,p-1\}$ 的 l 阶子群。元素 a^k的阶为 $\dfrac{l}{(k,l)}$。

5.5 置 换 群

定理 5.13 **n 元集合 $A=\{1,2,\cdots,n\}$ 上的全体置换构成集合 S_n。S_n 在合成运算之下构成一群，称之为 n 次对称群，其阶数为 $n!$**

证明 集合 A 上的置换是从 A 到 A 的双射。由于两个双射的合成映射仍是双射。所以 S_n 中的置换在合成运算之下是封闭的。并且映射的合成满足结合律。S_n 的单位元是恒同置换 $\sigma_I=\begin{pmatrix}1&2&\cdots n\\1&2&n\end{pmatrix}$。置换 σ 的逆元是它的逆置换 σ^{-1}。根据群的定义知 $\langle S_n,\cdot\rangle$ 是群。n 元置换共有 $n!$ 个。故 $|S_n|=n!$

定义 5.7 **集合 A 上的双射全体对于映射的合成运算构成群。该群叫作对称群。对称群的子群为置换群。**

由于置换的合成运算不满足交换律，所以置换群通常是非交换群。

例如，$S_2=\{\sigma_I,(12)\}$，$S_3=\{\sigma_I,(123),(132),(12),(13),(23)\}$。

例 1 图13中的等边三角形经旋转和反射使之三个顶点与原来的顶点重合在一起。一共有六种情况

$$\rho_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=\sigma_I,\qquad \mu_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(12),$$

$$\rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123),\qquad \mu_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(13),$$

$$\rho_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132),\qquad \mu_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(23),$$

其中 ρ_0,ρ_1,ρ_2 分别是绕等边三角形中心旋转 0°,120°,240° 的结果。μ_1,μ_2,μ_3 分别是对三个对称轴反射的结果。

令 $D_3=\{\rho_0,\rho_1,\rho_2,\mu_1,\mu_2,\mu_3\}$，$D_3$ 在合成运算之下形成一个置换群。它的乘法表如下：

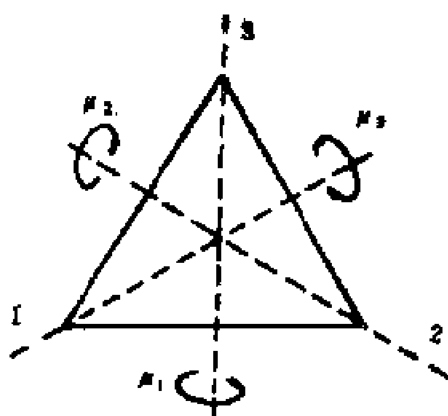


图 13

*	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

我们注意到 $\rho_1\cdot\mu_3=\mu_1$，$\mu_3\cdot\rho_1=\mu_2$，D_3 不是交换群，称它为三次二面体。$|D_3|=6$，恰好 $D_3=S_3$。

例 2 正方形通过旋转和反射使之顶点与原来顶点重合。共有如下 8 种情况：

$$\rho_0=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=\sigma_I,\qquad \mu_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(12)(34),$$

$$\rho_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1234),\quad \mu_2=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(14)(23),$$

$$\rho_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(13)(24),\qquad \delta_1=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}=(13),$$

$$\rho_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1432),\qquad \delta_2=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=(24).$$

其中 ρ_0，ρ_1，ρ_2，ρ_3 是正方形绕中心旋转 $0°$，$90°$，$180°$，$270°$ 的结果。μ_1，μ_2 是关于两个对边中点连线反射的结果。δ_1，δ_2 是关于两条对角线反射的结果(图14)。

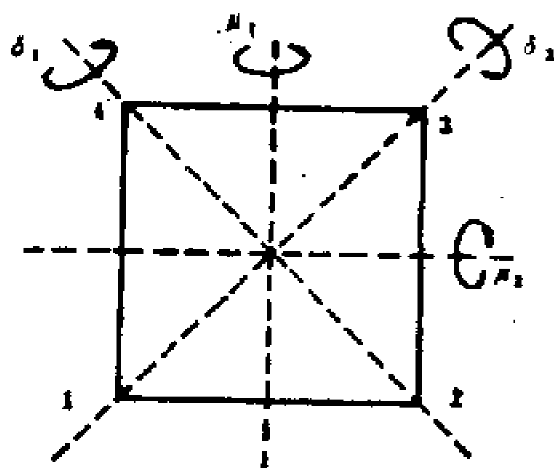


图 14

令 $D_4=\{\rho_0,\rho_1,\rho_2,\rho_3,\mu_1,\mu_2,\delta_1,\delta_2\}$，$D_4$ 在合成运算之下形成一个置换群。它的乘法表如下：

*	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

D_4 称为四次二面体。$|D_4|=8$。它是四次对称群 S_4 的子群。

例 3 证明$S_n=\langle(12),(13),\cdots,(1n)\rangle$，即对换(12)，(13)，…(1n)是$S_n$的生成元系。

证明 $\langle(12),(13),\cdots,(1n)\rangle$是由(12)，(13)，…，(1n)生成的群。由第三节例4知

$\langle(12),(13),\cdots,(1n)\rangle=\{\sigma_1\sigma_2\cdots\sigma_n \mid \sigma_i\in\{(12),(13),\cdots,(1n)\},1\leqslant i\leqslant n,n=1,2,\cdots\}$.

显然$\langle(12),(13),\cdots,(1n)\rangle\subseteq S_n$.

下面证明每个n元置换均可以写成(12)，(13)，…，(1n)这些基本元素的乘积。对n进行归纳证明。当$n=2$时，

$$\begin{pmatrix}1&2\\1&2\end{pmatrix}=(12)(12),\qquad \begin{pmatrix}1&2\\2&1\end{pmatrix}=(12),$$

该命题成立。假设$n=k$时命题成立，现$n=k+1$，

$$\sigma=\begin{pmatrix}1&2&\cdots&k&k+1\\ \sigma(1)&\sigma(2)&&\sigma(k)&\sigma(k+1)\end{pmatrix}.$$

有如下两种可能：

1° $\sigma(k+1)=k+1$，这时σ本身变成k元置换。由归纳假设命题成立。

2° $\sigma(k+1)\neq k+1$，必定存在l，$1\leqslant l\leqslant k$，$\sigma(l)=k+1$。用对换$(l\ k+1)$右乘σ得到σ_1

$$\begin{aligned}\sigma_1&=\sigma(l\quad k+1)\\&=\begin{pmatrix}1&2\cdots&l-1&l&l+1&\cdots&k+1\\ \sigma(1)&\sigma(2)&\sigma(l-1)&k+1&\sigma(l+1)&&\sigma(k+1)\end{pmatrix}(l\quad k+1)\\&=\begin{pmatrix}1&2&\cdots&l-1&l&l+1&\cdots&k&k+1\\ \sigma(1)&\sigma(2)&&\sigma(l-1)&\sigma(k+1)&\sigma(l+1)&\cdots&\sigma(k)&k+1\end{pmatrix},\end{aligned}$$

σ_1变为k元置换。由归纳假设σ_1可以写成(12)，(13)，…，(1n)的乘积。而$\sigma=\sigma_1(l\quad k+1)=\sigma_1(1\quad l)(1\quad k+1)(1\quad l)$，故$\sigma$可以写成(12)，(13)，…，(1k)，(1k+1)的乘积。命题对$n=k+1$也成立。**证毕**

例如$S_3=\{\sigma_I,(123),(132),(12),(13),(23)\}=\{(12)(12),$

(13)(12),(12)(13),(12),(13),(12)(13)(12)}。

5.6 群的同构

本节讨论两个群之间的关系。

我们在习题中曾经讨论过 $\langle S,*\rangle$，其中 $S=\{\alpha,\beta,\gamma,\delta\}$，乘法表为

*	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

$\langle S,*\rangle$ 是群。把该表的行与列适当地调换次序得到

*	γ	α	β	δ
γ	γ	α	β	δ
α	α	β	δ	γ
β	β	δ	γ	α
δ	δ	γ	α	β

再与第二节的 C_4 的乘法表比较，只要把 $\gamma,\alpha,\beta,\delta$ 分别换名为 $e,$ $,b,c$，它们是完全相同的。也就是说群 S 和群 C_4 的元素之间的有一种一一对应关系。我们研究群时并不关心元素本身是什么，关心的是元素与元素间的关系。所以，从这个意义上群 S 与群 C_4 是一回事。

为了刻划上述思想，我们引出同构的概念。

定义 5.9 $\langle G_1,*\rangle$ 与 $\langle G_2,\cdot\rangle$ 是两个群。如果存在着从集合 G_1 到集合 G_2 的双射 φ，对于任何 $a,b\in G_1$

$$\varphi(a*b)=\varphi(a)\cdot\varphi(b)。$$

则称群 G_1 与群 G_2 同构，记作 $G_1 \cong G_2$。双射 φ 称作同构映射。

φ 作为同构映射，除了要求它是双射外，还要求它保持运算。即 $\forall a, b \in G_1$，$\varphi(a*b) = \varphi(a) \cdot \varphi(b)$。形象地说，同构映射 φ 满足如下交换图表

$$\begin{array}{ccc} a, b & \xrightarrow{\ *\ } & a*b \\ \varphi \downarrow & & \downarrow \varphi \\ \varphi(a), \varphi(b) & \xrightarrow{\ \cdot\ } & \varphi(a*b) \end{array}$$

如果群 G_1 与群 G_2 同构，那么两个群的单位元之间以及元素和它的逆元之间有什么联系呢？这是下面定理要讨论的内容。

定理 5.14　φ 是从群 G_1 到群 G_2 的同构映射。e_1 和 e_2 分别是群 G_1 和 G_2 的单位元，必有 $\varphi(e_1) = e_2$，并且对任何 G_1 中的元素 a，$\varphi(a') = \varphi'(a)$。

证明　e_1 和 e_2 分别是群 G_1 和 G_2 的单位元。对任意 G_1 中的元素 a

$$\varphi(a) = \varphi(e_1 * a) = \varphi(e_1) \cdot \varphi(a)。$$

等式两边同时右乘 $\varphi'(a)$ 得到

$$e_2 = \varphi(a) \cdot \varphi'(a) = \varphi(e_1) \cdot \varphi(a) \cdot \varphi'(a) = \varphi(e_1),$$

即群 G_1 单位元 e_1 的同构映射象是 G_2 的单位元 e_2。

又对于 G_1 的任意元素 a，

$$\varphi'(a) = \varphi'(a) \cdot e_2 = \varphi'(a) \cdot \varphi(e_1) = \varphi'(a) \cdot \varphi(a) \cdot \varphi(a') = \varphi(a'),$$

即 G_1 任意元素 a 的逆元的象等于该元素同构映射象的逆元。

例 1　证明非负实数乘群与实数加群同构。

证明　$\langle R^+, \cdot \rangle$ 与 $\langle R, + \rangle$ 分别为非负实数乘群．与实数加群。$\varphi: R \to R^+$，$\varphi(x) = e^x$。显然 φ 是双射。对任意 $x, y \in R$，

$$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y),$$

故 φ 为同构映射。从而 $\langle R^+, \cdot \rangle \cong \langle R, + \rangle$。

这里要指出的是并非每个从 G_1 到 G_2 的双射都是同构映射。例如：$\psi: R \to R^+$，$\psi(x) = e^{x-1}$，显然 ψ 是双射。但是对任意 $x, y \in R$，

$$\psi(x+y)=e^{x+y-1},$$

$$\psi(x)\cdot\psi(y)=e^{x-1}\cdot e^{y-1}=e^{x+y-2},$$

故 ψ 不是从 R 到 R^+ 的同构映射。

例 2 在同构的意义下循环群 $G=\langle a\rangle$ 只有两类：若 a 是无限阶元，则 $G\cong\langle Z,+\rangle$。若 a 是 n 阶元，则 $G\cong Zn$。

证明 若循环群 $G=\langle a\rangle$ 的生成元 a 是无限阶元，对任何 $m_1\neq m_2$ 均有 $a^{m_1}\neq a^{m_2}$。f 是从 G 到整数集合 Z 的映射，$f:G\to Z$，$f(a^m)=m$。显然 f 是双射。对任意 $a^{m_1},a^{m_2}\in G$，

$$f(a^{m_1}*a^{m_2})=f(a^{m_1+m_2})=m_1+m_2=f(a^{m_1})+f(a^{m_2})。$$

f 是同构映射，故 $G\cong\langle Z,+\rangle$。

若生成元 a 是 n 阶元，则 $G=\{a^0,a^1,a^2,\cdots,a^{n-1}\}$。$f$ 是从 G 到模 n 同余类集合 Zn 的映射，$f:G\to Zn$，$f(a^i)=[i]$。显然 f 是双射。对任意 a^i，$a^j\in G$，

$$f(a^i*a^j)=f(a^{i+j})=[i+j]=[i]+[j]=f(a^i)+f(a^j)。$$

f 是同构映射，故 $G\cong\langle Zn,+\rangle$。

例 3 任意一个群都与一个置换群同构。

证明 对于任意群 $\langle G,*\rangle$ 构造一个新的集合

$$G'=\{f_a|a\in G,f_a:G\to G,f_a(x)=a*x\}，$$

容易证明 f_a 是 G 上的双射。G' 上的运算·是映射的合成运算。

$$(f_a\cdot f_b)(x)=f_a(b*x)=(a*b)*x=f_{a*b}(x),$$

即 $f_a\cdot f_b=f_{a*b}$。该运算在 G' 中封闭并且满足结合律。f_e 是 G' 的单位元，$f_{a'}$ 是 f_a 的逆元，从而 $\langle G',\cdot\rangle$ 是置换群。

在群 G 与 G' 之间定义映射 h：$G\to G'$，$h(a)=f_a$，显然 h 是双射。对任意 $a,b\in G$，

$$h(a*b)=f_{a*b}=f_a\cdot f_b=h(a)\cdot h(b),$$

故 h 是同构映射。从而 $G\cong G'$。**证毕。**

例 4 求出与 n 阶循环群同构的置换群。

解 令 $G=\langle a\rangle$ 是循环群，$f:G\to G'$ 是同构映射。任取 $x\in G'$，必存在 $g=a^i\in G$ 使

$$x=f(g)=f(a^t)=(f(a))^t.$$

这说明 G' 是以 $f(a)$ 为生成元的循环群．现 G 是 n 阶循环群，$G=\{a^0,a^1,\cdots,a^{n-1}\}$，从例 3 可知 $G'=\{f_{a^0},f_{a^1},\cdots,f_{a^{n-1}}\}$也是 n 阶循环群。其生成元是 f_a，它对应 G 上的长为 n 的轮换 $(a^0,a^1,\cdots,a^{n-1})$。令 $G''=\langle(a^0,a^1,\cdots,a^{n-1})\rangle$，则 $G\cong G''$。

定理 5.15 $\langle G,*\rangle$ **为群，另有一个集合** G'，$\cdot$ **是** G' **上的运算．如果存在从** G **到** G' **上的双射** f，**对** G **中的任意元素** a,b **有** $f(a*b)=f(a)\cdot f(b)$。**那么** $\langle G',\cdot\rangle$ **也是群，并且**$G\cong G'$。

证明 任取 $x,y\in G'$，f是从 G 到 G' 的满射，存在 $a,b\in G$ 使得 $f(a)=x,f(b)=y$。由于 f 保持运算

$$x\cdot y=f(a)\cdot f(b)=f(a*b)\in G',$$

可知运算 $\cdot$ 在 G' 是封闭的，任取 $x,y,z\in G'$。对于满射 f 在 G 中有原象。$f(a)=x$, $f(b)=y$, $f(c)=z$。

$$\begin{aligned}(x\cdot y)\cdot z&=(f(a)\cdot f(b))\cdot f(c)=f((a*b)*c).\\&=f(a*(b*c))=f(a)\cdot(f(b)\cdot f(c))=x\cdot(y\cdot z),\end{aligned}$$

即 G' 中运算 $\cdot$ 满足结合律。容易看出 $f(e)$ 是 G' 的单位元。任取 $x\in G'$，$a\in G$ 是它的原象，易知 $f(a')\in G'$ 是 x 的逆元。

综上知 $\langle G',\cdot\rangle$ 是群。f 就是从 G 到 G' 的同构映射，从而 $G\cong G'$。

习 题

1. 如下代数系统 $\langle S,*\rangle$ 哪些是群？如果是群，它是否是交换群？指出它的单位元以及如何计算逆元。

(1) $S=\{z\mid z\in C, |z|=1\}$，其中 C 是复数集合．$*$ 是普通的复数加法。

(2) $S=\{a+b\sqrt{2}\mid a,b\in Q\}$，其中 Q 是有理数集合．$*$ 是普通的加法。

(3)

$$S=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\},$$

$*$ 是矩阵乘法。

(4) $S=\{\alpha,\beta,\gamma,\delta\}$,

$*$	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

(5) $S=\mathrm{R}-\{0\}$ 是非零实数集合，S 上定义运算 $*$：

$$x*y=\begin{cases} x\cdot y, & x>0, \\ x/y, & x<0. \end{cases}$$

(6) p 为素数，$S=\{1,2,\cdots,p-1\}$。S 上定义运算 $*$：

$$a*b=c \Leftrightarrow a\cdot b\equiv c \pmod{p}.$$

2. 令 $S=\mathrm{R}-\{-1\}$，S 上定义运算 $*$：

$$a*b=a+b+ab.$$

(1) 证明 $\langle S,*\rangle$ 是群.

(2) 在 S 中求解方程 $2*x*3=7$.

3. 在群 G 中，如果对 G 有任意元素 a 均有 $a^2=e$，证明 G 必是交换群.

4. G 是交换群当且仅当对 G 中任意元素 a, b, $(a*b)^2=a^2*b^2$.

5. g 是群 G 中的任意元素，那么，

(1) g 与它的逆元 g' 同阶.

(2) $(g^k)'=(g')^k$.

6. a 与 b 是群 G 中的两个任意元素。证明 $a*b$ 与 $b*a$ 是同阶的.

7. 如果群 G 中只有一个二阶元 a，那么 a 与 G 中任意元素都是交换的，即 $\forall x\in G$, $a*x=x*a$.

8. G 是群，G 中的元素个数为偶数，证明存在 $a\in G$，a 是二阶元.

9. H 是群 G 的非空子集，$\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的子群当且仅当 $\forall a,b\in H, a*b'\in H$.

10. G 是群.

$$H=\{a|a\in G, \forall g\in G, a*g=g*a\},$$

称为群 G 的中心. 证明：$\langle H,*\rangle$ 是 $\langle G,*\rangle$ 的子群.

11. H, K 是群 G 的子群. 证明 $H\cap K$ 也是 G 的子群. $H\cup K$ 是 G 的子群吗? 证明你的结论.

12. 找出 K_4 群的所有子群.

13. 令 $G=\{f_{a,b}|f_{a,b}: \mathrm{Q}\to\mathrm{Q}, f(x)=ax+b, a\neq 0, a, b\in\mathrm{Q}\}$，$G$ 对合成运算构成群. 证明 $H=\{f_{1,b}|b\in\mathrm{Q}\}$ 是 G 的子群.

14. 指出下列群中哪个是循环群? 对循环群写出它的全部生成元.

(1) $G_1=\langle\mathrm{Q},+\rangle$.

(2) $G_2=\langle 6\mathbf{Z},+\rangle$.

(3) $G_3=\langle\{6^n|n\in\mathbf{Z}\},\cdot\rangle$.

15. G是6阶循环群，找出G的全部生成元并列出G的所有子群。

16. 证明：只有一个生成元的循环群至多含有两个元素。

17. 如果n阶群G的某个元素g是n阶的，那么G是由g生成的循环群。

18. G是n阶循环群，d是n的因子，G存在且仅存在一个d阶子群。

19. 找出S_3的所有子群。

20. A_4是全体4元偶置换构成的群，请列出它的全部元素。

21. Sn $(n\geqslant 2)$的每个子群或者全部由偶置换构成，或者其中奇、偶置换各占一半。

22. 证明整数加群与偶数加群同构。

23. 证明：群的同构关系是一种等价关系。

24. 找出所有与K_4群同构的S_n的子群。

25. 证明：无限循环群的子群，除$\{e\}$以外都是无限循环群。

26. 在群$\langle G,*\rangle$中定义新的二元运算$\cdot$，

$$a\cdot b=b*a.$$

证明$\langle G,\cdot\rangle$是群，并且$\langle G,*\rangle$与$\langle G,\cdot\rangle$同构.

6 商　群

为了深入探讨群的结构，需要进一步研究子群的作用。

6.1 陪集与Lagrange定理

定义 6.1 H 是 G 的子群。在 G 上定义模 H 同余关系，$\forall a, b\in G$，如果 $a*b'\in H$，则称 a 与 b 模 H 同余，记作 $a\equiv b(\mathrm{mod}\ H)$。

定理 6.1 模 H 同余关系是 G 上的等价关系。对于 G 中元素 a，a 所在的等价类为

$$Ha=\{h*a\mid h\in H\},$$

称为 G 中 H 的右陪集。元素 a 是陪集 Ha 的代表元。

证明 任取 $a\in G$，$a*a'=e\in H$，故 $a\equiv a(\mathrm{mod}\ H)$。模 H 同余关系是自反的。如果 $a,b\in G$，$a\equiv b(\mathrm{mod}\ H)$，即 $a*b'\in H$。因 H 是群，$(a*b')'=b*a'\in H$。故 $b\equiv a(\mathrm{mod}\ H)$。模 H 同余关系是对称的。如果 $a, b, c\in G$，$a\equiv b(\mathrm{mod}\ H)$，$b\equiv c(\mathrm{mod}\ H)$，即 $a*b'\in H$，$b*c'\in H$。H 是 G 的子群，H 对群 G 的运算 $*$ 封闭，$(a*b')*(b*c')=a*c'\in H$，故 $a\equiv c(\mathrm{mod}\ H)$。模 H 同余关系是传递的。综上分析知模 H 同余关系是 G 上的等价关系。

G 中元素 a 所在的等价类

$$[a]=\{b\mid b\in G, b*a'\in H\}$$
$$=\{h*a\mid h\in H\}=Ha.$$

显然 $a\in Ha$，a 是该等价类的代表元。证毕。

模 H 同余关系有如下性质：

1° $He=H$。

2° $a \equiv b \pmod H \Longleftrightarrow Ha = Hb$.

3° $a \in H \Longleftrightarrow Ha = H$.

例 1 非零有理数乘法群 $\langle Q^*, \cdot \rangle$，$H = \{-1, 1\} \subset Q^*$，是该乘法群的子群。$Q^*$ 中元素 a 所在的右陪集 $Ha = \{a, -a\}$。当 $a \equiv b \pmod H$ 时，$b = \pm a$，显然 $Ha = Hb$。

例 2 三次二面体群 $\langle D_3, \cdot \rangle$，$H = \{\rho_0, \rho_1, \rho_2\}$ 是 D_3 的子群。因 $\rho_i \in H$，$0 \leqslant i \leqslant 2$，故 $H\rho_0 = H\rho_1 = H\rho_2 = H$。又因 $u_i * u_j' \in H$，$1 \leqslant i, j \leqslant 3$，故 $Hu_1 = Hu_2 = Hu_3 = \{u_1, u_2, u_3\}$。$H$ 有两个不同的右陪集 H 和 Hu_1，$D_3 = H \cup Hu_1$ 且 $H \cap Hu_1 = \varnothing$。

例 3 G 是以 g 为生成元的 9 阶循环群，$G = \{g^0, g^1, \cdots, g^8\}$，$g^9 = e$。$H = \{g^0, g^3, g^6\}$ 是 G 的 3 阶子群。

$$Hg^0 = Hg^3 = Hg^6 = \{g^0, g^3, g^6\} = H,$$
$$Hg^1 = Hg^4 = Hg^7 = \{g^1, g^4, g^7\},$$
$$Hg^2 = Hg^5 = Hg^8 = \{g^2, g^5, g^8\}.$$

H 有三个不同的右陪集 H，Hg，Hg^2。$G = H \cup Hg \cup Hg^2$，且这些右陪集两两非交。

对于群 G 的子群 H 也可以定义它的左陪集，先在 G 上定义等价关系。$\forall a, b \in G$，

$$a \equiv b \pmod H \Longleftrightarrow a' * b \in H.$$

G 中元素 a 所在的等价类 $[a] = \{b \mid b \in G,\ a' * b \in H\} = \{a * h \mid h \in H\} = aH$，称为 a 所在的左陪集。

定理 6.2 **H 是群 G 的子群，H 的所有左陪集集合 $S_L = \{aH \mid a \in G\}$ 和所有右陪集集合 $S_R = \{Ha \mid a \in G\}$ 是等势的。**

证明 令 $f: S_L \to S_R$，$f(aH) = Ha'$。这里首先要说明该映射与代表元选取无关，即若 $aH = bH$，必有 $Ha' = Hb'$。由 $aH = bH$ 知 $a' * b \in H$，H 是群，$(a' * b)' = b' * (a')' \in H$，从而 $Ha' = Hb'$。显然 f 是满射。如果 a_1H，$a_2H \in S_L$ 都是 Ha 的原象，$f(a_1H) = f(a_2H) = Ha$，得出 $Ha_1' = Ha_2'$，故有 $(a_1') * (a_2')' = a_1' * a_2 \in H$。由此可知 $a_1H = a_2H$，这说明 f 是单射。

综上分析，在 S_L 与 S_R 之间存在着一个双射. 故 S_L 与 S_R 等势. **证毕。**

注意：在上定理证明中定义的映射是 $f(aH)=Ha'$，而不是 Ha。后者它不是映射。当 $aH=bH$ 时，不能保证 $Ha=Hb$。

定义 6.2　群 G 关于它的子群 H 的左(右)陪集个数叫做 H 在 G 中的指数，记为 $[G:H]$。

定理 6.3　(Lagrange 定理)

若 G 是有限群，H 是 G 的子群，那么

$$|G|=[G:H]\,|H|.$$

证明　Ha 是 G 中 H 的一个右陪集。定义映射 $f: H\to Ha$，$f(h)=h*a$，显然 f 是双射. G 是有限群，H 是 G 的子群，所以 H 也是有限群，得出 $|H|=|Ha|$。由定理 6.1 知，G 中 H 的右陪集全体构成 G 的一个分划，令 G 关于子群 H 的右陪集个数 $[G:H]=k$，k 个不同的右陪集的代表元分别为 $a_1, a_2, \cdots, a_k$，那么 $G=Ha_1\cup Ha_2\cup\cdots\cup Ha_k$，其中 $Ha_i\cap Ha_j=\varnothing$，$(i\neq j)$。从而

$$|G|=|Ha_1|+|Ha_2|+\cdots+|Ha_k|$$
$$=k\cdot|H|=[G:H]\cdot|H|.$$

证毕。

由此定理可以得到两个非常有用的推论。

推论 6.1　有限群 G 中元素的阶是 $|G|$ 的因子。

明证　在有限群中所有元素的阶必然是有限的。设 G 中的元素 a 的阶为 m，令 $H=\{a^0, a^1, \cdots, a^{m-1}\}$，显然 H 是 G 的 m 阶子群。由 Lagrange 定理知 $|G|=[G:H]\cdot|H|=[G:H]\cdot m$。故 $m\mid|G|$。**证毕。**

推论 6.2　素数阶群都是循环群。

证明　设 G 是 p 阶群，p 是素数。它的因子只有 1 和 p。由推论 6.1 知 G 中元素的阶是 1 或者 p。显然群 G 的单位元的阶为 1，非单位元元素 a 的阶为 p，从而 $G=\langle a\rangle$。

例 1　证明 4 阶群 G 或者是 4 阶循环群 C_4 或者是 Klein-4

群 K_4。

证明 4阶群 G 中元素的阶可能为 1, 2, 4。如果 G 中包括 4 阶元 a, 那么 $G=\langle a\rangle=\{a^0, a^1, a^2, a^3\}$, 即 G 是 4 阶循环群 C_4。如果 G 中没有 4 阶元,那么除单位元 e 外,其它元素均是 2 阶元,即 $G=\{e, a, b, c\}$, $a^2=b^2=c^2=e$。由前面的习题知该群必是交换群。$a*b$ 不能是 a, b, e, 否则推出 $b=e$, $a=e$, $a=b$。从而 $a*b=c$。同理可知 $a*c=b$, $b*c=a$。据此得出该群的乘法表

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

故 G 是 Klein-4 群 K_4。

例 2 G 是 6 阶群, G 至少含有一个 3 阶子群。

证明 G 是 6 阶群。G 中元素的阶可能是 1, 2, 3, 6。如果 G 中有 3 阶元 a, 那么$\langle a\rangle$就是 G 的 3 阶子群。如果 G 中有 6 阶元 a, 那么$\langle a^2\rangle$为 G 的 3 阶子群。下面证明 G 中不可能既无 3 阶元也无 6 阶元。也就是说 G 中不可能除掉单位元 e 外都是 2 阶元。用反证法,假设 $G=\{e, a, b, c, d, f\}$, 且 $a^2=b^2=c^2=d^2=f^2=e$。由于 $a*b$ 不可为 a, b, e,取$K=\{e,a,b, a*b\}$,其中$a*b\in\{c, d, f\}$,显然 K 是 Klein-4 群。而 $K\subseteq G$。故 K 是 G 的子群。$|K|=4$, 而 $4\nmid 6$,与 Lagrange 定理矛盾。故不可。综上知六阶群必有三阶子群。**证毕**。

6.2 正规子群与商群

本节介绍一类特殊的子群——正规子群。

定义 6.3 H **是群** G **的子群。如果对所有的** G **中元素** g **和** H **中元素** h **都有** $g'*h*g\in H$, **那么称** H **是** G **的正规子群,并记为**$H\lhd G$。

定理 6.4 **H是群 G 的子群，H 是 G 的正规子群当且仅当对任意 G 中元素 g，$Hg=gH$。**

证明 若 H 是 G 的正规子群. 任取 $x\in gH$，存在 $h_1\in H$ 使 $x=g*h_1$。而$x=(g')'*h_1*g'*g$，由正规子群的定义，$(g')'*h_1*g'\in H$，故 $x\in Hg$，于是 $gH\subseteq Hg$。反过来，任取 $y\in Hg$，存在 $h_2\in H$ 使 $y=h_2*g$，而 $y=g*g'*h_2*g$，由正规子群的定义 $g'*h_2*g\in H$，故 $y\in gH$。于是 $Hg\subseteq gH$。综上知 $Hg=gH$。

又若对任意 G 中元素 g 均有 $Hg=gH$，任取 $h_3\in H$，必存在 $h_4\in H$ 使 $h_3*g=g*h_4$，于是 $g'*h_3*g=h_4\in H$。从而 H 是 G 的正规子群。**证毕**

例 1 三次二面体 D_3 的子群 $H=\{\rho_0, \rho_1, \rho_2\}$ 是正规子群。

$$\rho_0H=\rho_1H=\rho_2H=H\rho_0=H\rho_1=H\rho_2=\{\rho_0,\rho_1\rho_2\},$$

$$\mu_1H=\mu_2H=\mu_3H=H\mu_1=H\mu_2=H\mu_3=\{\mu_1,\mu_2,\mu_3\}.$$

$\tilde{H}=\{\rho_0,\mu_1\}$是 D_3 的子群，但不是正规子群。例如

$$\mu_2\tilde{H}=\{\mu_2, \rho_1\},$$

$$\tilde{H}\mu_2=\{\mu_2,\rho_2\}.$$

$\mu_2\tilde{H}\neq\tilde{H}\mu_2$。

例 2 指数为 2 的子群是正规子群。

证明 H 是群 G 的子群且 $[G:H]=2$，即 $G=H\cup Ha_1$，其中 $a_1\notin H$，并且 $H\cap Ha_1=\varnothing$。我们任取群 G 的元素 a，有两种可能性：若 $a\in H$，由于 $aH=H$，$Ha=H$，故 $aH=Ha$；若$a\notin H$，$G=H\cup Ha=H\cup aH$。$Ha=G-H=aH$。所以不管是哪种情况均有 $aH=Ha$。H 是 G 的正规子群。**证毕。**

显然交换群的任何子群都是正规子群。

下面研究在 G 中 H 的所有右陪集构成的集合上的运算及相应的代数结构。

定义 6.4 **A,B 是群 G 的非空子集，定义**

$$A\cdot B=\{a*b\,|\,a\in A,\ b\in B\}.$$

该运算满足结合律，任取 $x\in A\cdot(B\cdot C)$，存在 $a\in A$，$b\in B$，

$c \in C$ 使 $x = a*(b*c)$。群 G 中乘法满足结合律 $x = (a*b)*c$，故 $x \in (A \cdot B) \cdot C$。从而 $A \cdot (B \cdot C) \subseteq (A \cdot B) \cdot C$。同理也可证明 $(A \cdot B) \cdot C \subseteq A \cdot (B \cdot C)$，最后得到 $A \cdot (B \cdot C) = (A \cdot B) \cdot C$。

定理 6.5 **N 是群 G 的正规子群，$\langle \{Ng \mid g \in \}, G \cdot \rangle$ 是群。称为 G 模 N 的商群，记为 G/N。**

证明 首先研究两个正规子群的右陪集怎样做乘法

$$Ng_1 \cdot Ng_2 = \{(n_1 * g_1)*(n_2 * g_2) \mid n_1, n_2 \in N\}。$$

因 N 是 G 的正规子群，对于 G 中元素 g_1 有 $g_1 N = N g_1$。$g_1 * n_2 \in g_1 N$，那么存在 $n_3 \in N$ 使 $g_1 * n_2 = n_3 * g_1$，代入上式

$$\begin{aligned} Ng_1 \cdot Ng_2 &= \{n_1 * (n_3 * g_1) * g_2 \mid n_1, n_3 \in N\} \\ &= \{n * (g_1 * g_2) \mid n \in N\} \\ &= N g_1 * g_2。\end{aligned}$$

这里定义的正规子群右陪集间的乘法运算与右陪集代表元的选取是无关的。这是因为，如果 $Ng_1 = Na_1$，$Ng_2 = Na_2$，即 $g_1 * a_1'$，$g_2 a_2' \in N$，那么

$$(g_1 * g_2)*(a_1 * a_2)' = g_1 * (g_2 * a_2') * a_1'。$$

令 $n_1 = g_2 * a_2'$，$n_1 * a_1' = a_1' * n_2$，$n_3 = g_1 * a_1'$，

$$(g_1 * g_2)*(a_1 * a_2)' = n_3 * n_1 \in N。$$

于是 $Ng_1 * g_2 = Na_1 * a_2$。

在集合 $\{Ng \mid g \in G\}$ 上的乘法运算显然是封闭的。并且满足结合律。$N = Ne$ 是单位元，Ng' 是 Ng 的逆元。所以 $\langle \{Ng \mid g \in G\}, \cdot \rangle$ 是群。

当 G 是有限群时，G 模 N 的商群 G/N 中元素个数就是 N 在 G 中的指数，故

$$|G/N| = |G| / |N|。$$

例 1 整数加群 $\langle Z, + \rangle$ 是交换群。每个子群都是正规子群。Z 模正规子群 $\langle n \rangle = \{kn \mid k \in Z\} = nZ$ 的商群

$$Z/nZ = \{nZ, 1 + nZ, \cdots, (n-1) + nZ\},$$

若映射 $f: Z/nZ \to Z_n$，$f(i + nZ) = [i]$，显然 f 是双射。故

$$\mathbf{Z}/n\mathbf{Z}\cong\mathbf{Z}_n.$$

例 2 三次二面体 D_3 中，子群 $H=\{\rho_0,\rho_1,\rho_2\}$ 的指数为 2。H 是 D_3 的正规子群，D_3 模 H 的商群

$$D_3/H=\{H,(12)H\}$$

是二阶循环群。

例 3 G 是有限交换群。素数 p 是 $|G|$ 的因子，那么群 G 中必有一个 p 阶元。

证明 我们对群 G 的阶数进行归纳证明。当 $|G|=2$ 时，$G=\{e,a\}$ 且 $a^2=e$。素数 $2\mid|G|$。a 是二阶元。命题成立。假设 $|G|<k$ 时，命题成立。现 $|G|=k$，某素数 $p\mid k$。任取 G 的某个非单位元素 g，它的阶为 t，显然 $t\mid k$ 且 $t>1$。如果 $p\mid t$，即 $t=rp$，则 g^r 是 G 中的 p 阶元。如果 $p\nmid t$，考虑 G 模正规子群 $\langle g\rangle$ 的商群 $G/\langle g\rangle$。

$$|G/\langle g\rangle|=|G|/t<|G|=k,$$

$G/\langle g\rangle$ 仍是有限交换群。由于 $p\mid k, p\nmid t$，故 $p\mid|G/\langle g\rangle|$。由归纳假设知在 $G/\langle g\rangle$ 中有 p 阶元 $a\langle g\rangle$。假设 a 在 G 中的阶为 u，显然有 $(a\langle g\rangle)^u=\langle g\rangle$。从而 $p\mid u$。由前面讨论知 $a^{u/p}$ 是 G 中的 p 阶元。命题对 $|G|=k$ 也成立。**证毕。**

一般地，n 阶群 G，对 n 的因子 d，在 G 中不一定有 d 阶子群。例如：全体四元偶置换构成 A_4，$|A_4|=12$。6 是 12 的因子，但 A_4 没有 6 阶子群，这是因为 A_4 中有 1 个 1 阶元，8 个 3 阶元，3 个 2 阶元。若 H 是 A_4 的 6 阶子群，因 2 阶元只有 3 个，故 H 中至少有一个三阶元，不妨假设是 $(a,b,c)\in H$。三阶元的逆元仍是三阶元，故三阶元必须成对出现。单位元 $e\in H$，所以 H 中至少有一个二阶元，不妨假设是 $(ab)(cd)\in H$。由 $(a,b,c)\in H$，$(ab)(cd)\in H$ 推出 $(abc)'=(acb)\in H$。$(abc)(ab)(cd)=(acd)\in H$，$(acd)'=(adc)\in H$，$(ab)(cd)(abc)=(bdc)\in H$，$(bdc)'=(bcd)\in H$，…，H 中的元素个数已超出 6 个，与 H 是 A_4 的 6 阶子群矛盾。所以 A_4 没有 6 阶子群。

6.3 群的同态

本节继续讨论两个群之间的关系。

定义 6.5 在群$\langle G_1,*\rangle$和$\langle G_2,\cdot\rangle$之间存在映射$f:G_1\to G_2$，对任意$a,b\in G$，$f(a*b)=f(a)\cdot f(b)$，则称f是从G_1到G_2的同态映射（简称同态）。如果f是满射（单射，双射），则称f是满同态映射（单一同态映射，同构映射）。

若f是从群G_1到G_2的同态映射，G_1，G_2的单位元分别是e_1和e_2，那么$f(e_1)=e_2$。对任意$a\in G$，$f(a')=(f(a))'$。此结论证明方法与群同构映射相应性质证明方法相同。

定义 6.6 f是从G_1到G_2的群同态映射，f的核是G_1中通过f映到G_2的单位元e_2的那些元素组成的集合，记为$\mathrm{Ker}\,f$

$$\mathrm{Ker}\,f=\{a\mid a\in G_1,\ f(a)=e_2\}.$$

定理 6.6 f是从G_1到G_2的群同态映射。

1° $\mathrm{Ker}\,f$是群G_1的正规子群。

2° f为单射当且仅当$\mathrm{Ker}\,f=\{e_1\}$。

证明

1° f是从G_1到G_2的群同态映射。由于$f(e_1)=e_2$，$e_1\in\mathrm{Ker}\,f$，所以$\mathrm{Ker}\,f$是G_1的非空子集。任取g_1，$g_2\in\mathrm{Ker}\,f$，$f(g_1)=f(g_2)=e_2$，而

$$f(g_1*g_2)=f(g_1)\cdot f(g_2)=e_2\cdot e_2=e_2,$$
$$f(g_1')=(f(g_1))'=e_2'=e_2,$$

故$g_1*g_2\in\mathrm{Ker}\,f$，$g_1'\in\mathrm{Ker}\,f$，从而$\mathrm{Ker}\,f$是$G_1$的子群，任取$g\in G_1$，$k\in\mathrm{Ker}\,f$，

$$\begin{aligned}f(g'*k*g)&=(f(g))'\cdot f(k)\cdot f(g)\\&=(f(g))'\cdot e_2\cdot f(g)=e_2,\end{aligned}$$

故$g'*k*g\in\mathrm{Ker}\,f$。$\mathrm{Ker}\,f$是G_1的正规子群。

2° 当f为单射时，只有e_1的象为e_2，故$\mathrm{Ker}\,f=\{e_1\}$，反过

来，当 $\mathrm{Ker}\, f=\{e_1\}$ 时，如果存在 $g_2\in G_2$，它有两个不同的原象 $g_{11}, g_{12}\in G_1$，$g_{11}\neq g_{12}$，$f(g_{11})=f(g_{12})=g_2$。

$$f(g_{11}*g'_{12})=f(g_{11})\cdot(f(g_{12}))'=g_2\cdot g'_2=e_2,$$

那么 $g_{11}*g'_{12}\in \mathrm{Ker}\, f=\{e_1\}$，即 $g_{11}*g'_{12}=e_1$。从而得到 $g_{11}=g_{12}$，矛盾。这说明如果 G_2 中的元素有原象，那么原象是唯一的，所以 f 是单射。

例 1 G_1 和 G_2 是任意两个群，令 $f:G_1\to G_2$，对任意 $g\in G_1$，$f(g)=e_2$。任取 $g_1, g_2\in G_1$，

$$f(g_1*g_2)=e_2=e_2\cdot e_2=f(g_1)\cdot f(g_2),$$

f 是群同态映射。$\mathrm{Ker}\, f=G_1$，我们称这个特殊的同态映射为零同态映射。

例 2 $G_1=\langle Z, +\rangle$，$G_2=\langle C, \cdot\rangle$，令 $f:Z\to C$，$f(m)=i^m$。$f(k+l)=i^{k+l}=i^k\cdot i^l=f(k)\cdot f(l)$。$f$ 是从 G_1 到 G_2 的同态映射。$\mathrm{Ker}\, f=\{n\mid i^n=1\}=\{4m\mid m\in Z\}$。$f$ 的象集 $\mathrm{Im}\, f=\{1, -1, i, -i\}$。

定理 6.7 f **是群** G_1 **到** G_2 **的一个同态映射。**

1° 若 $H_1\leqslant G_1$，**则** $f(H_1)\leqslant G_2$。**特别地**，$f(G_1)\leqslant G_2$。

2° 若 $H_1\lhd G_1$，**则** $f(H_1)\lhd f(G_1)$。

3° 若 $H_2\leqslant f(G_1)$，**则** $f^{-1}(H_2)\leqslant G_1$。

4° 若 $H_2\lhd f(G_1)$，**则** $f^{-1}(H_2)\lhd G_1$ **且** $G_1/f^{-1}(H_2)\cong f(G_1)/H_2$。

证明 这里只证 2°，3°，其它留作习题。

2° H_1 是 G_1 的正规子群，由 1° 知 $f(H_1)\leqslant G_2$。而 $f(H_1)\subseteq f(G_1)\subseteq G_2$，$f(G_1)$ 为群，故 $f(H_1)$ 是 $f(G_1)$ 的子群。任取 $y\in (G_1)$，$x\in f(H_1)$，存在 $g\in G_1$，$h\in H_1$ 使 $f(g)=y$，$f(h)=x$。

$$y'\cdot x\cdot y=f(g')\cdot f(h)\cdot f(g)=f(g'*h*g),$$

由于 H_1 是 G_1 的正规子群，$g'*h*g\in H_1$。故 $y'\cdot x\cdot y\in f(H_1)$，$f(H_1)$ 是 $f(G_1)$ 的正规子群。

3° H_2 是 $f(G_1)$ 的子群。$f^{-1}(H_2)=\{x\mid x\in G_1, f(x)\in H_2\}$

$\subseteq G_1$。$f(e_1)=e_2\in H_2$，显然 $e_1\in f^{-1}(H_2)$。$f^{-1}(H_2)$ 是 G_2 的非空子集。若 $x_1,x_2\in f^{-1}(H_2)$，存在 $h_1,h_2\in H_2$ 使 $f(x_1)=h_1,f(x_2)=h_2$。

$$f(x_1*x_2)=f(x_1)\cdot f(x_2)=h_1\cdot h_2\in H_2,$$
$$f(x_1')=(f(x_1))'=h_1'\in H_2。$$

可知 $x_1*x_2\in f^{-1}(H_2)$，$x_1'\in f^{-1}(H_2)$。从而 $f^{-1}(H_1)$ 是 G_1 的子群。

定理 6.8 **f 是从 G_1 到 G_2 的群同态映射，对任意 $a\in G_1$，$f(f(a))=a\,\mathrm{Ker}\,f$。**

证明 任取 $a\in G_1$，f 是从 G_1 到 G_2 的群同态映射，$f(a)\in G_2$。由 f^{-1} 定义知 $f^{-1}(f(a))=\{x|x\in G_1,\ f(x)=f(a)\}$。任取 $x\in f^{-1}(f(a))$，$f(a'*x)=f(a')\cdot f(x)=(f(a))'\cdot f(a)=e_2$，故 $a'*x\in \mathrm{Ker}\,f$，即 $x\in a\,\mathrm{Ker}\,f$。从而得出 $f^{-1}(f(a))\subseteq a\,\mathrm{Ker}\,f$。又任取 $y'\in a\,\mathrm{Ker}\,f$，存在 $k\in \mathrm{Ker}\,f$ 使 $y=a*k$，$f(y)=f(a)\cdot f(k)=f(a)\cdot e_2=f(a)$，所以 $y\in f^{-1}(f(a))$。又得出 $a\,\mathrm{Ker}\,f\subseteq f^{-1}(f(a))$ 综上分析知

$$f^{-1}(f(a))=a\,\mathrm{Ker}\,f。$$

证毕。

这个定理说明了，若 f 是从 G_1 到 G_2 的满同态，则 G_2 中每个元素的原象集正好是 f 的同态核 $\mathrm{Ker}\,f$ 的一个陪集。据此，我们可以在 $G_1/\mathrm{Ker}\,f$ 和 G_2 之间建立起一个一一对应关系。

定理 6·9 （群同态基本定理）

群 G_1 的任何商群都是 G_1 的同态象。若 G_2 是 G_1 的同态象，则 $G_1/\mathrm{Ker}\,f\cong G_2$。

证明 设 H 是群 G_1 的正规子群。定义 $\varphi:G_1\to G_1/H,\varphi(a)=aH$。显然 φ 是满同态映射，$\varphi(G_1)=G_1/H$，这就证明了群 G_1 的任何商群都是 G_1 的同态象。

若 G_2 是 G_1 的同态象，即 $f:G_1\to G_2$，$f(G_1)=G_2$。定义 $\bar{f}$: $G_1/\mathrm{Ker}\,f\to G_2$，$\bar{f}(a\,\mathrm{Ker}\,f)=f(a)$。首先要说明 $\bar{f}$ 是映射，就是

说如果 $a_1\,\mathrm{Ker}\,f=a_2\,\mathrm{Ker}\,f$，那么 $a_1'*a_2\in \mathrm{Ker}\,f$。而 $(f(a_1))'\cdot f(a_2)=f(a_1'*a_2)=e_2$，得出 $f(a_1)=f(a_2)$。即映射 $\bar{f}$ 与代表元选取无关。

任取 $y\in G_2=f(G_1)$，存在 $a\in G_1$ 使 $y=f(a)$，那么 $a\,\mathrm{Ker}\,f\in G_1/\mathrm{Ker}\,f$ 是 y 的原象。又若 $a_1\,\mathrm{Ker}\,f$，$a_2\,\mathrm{Ker}\,f\in G_1/\mathrm{Ker}\,f$ 都是 $y\in f(G_1)$ 的原象，那么 $f(a_1)=f(a_2)$。而 $f(a_1'*a_2)=(f(a_1))'\cdot f(a_2)=e_2$，故 $a_1'*a_2\in \mathrm{Ker}\,f$，即 $a_1\,\mathrm{Ker}\,f=a_2\,\mathrm{Ker}\,f$。由上面分析知 $\bar{f}$ 是双射。

$$\begin{aligned}\bar{f}(a\,\mathrm{Ker}\,f\cdot b\,\mathrm{Ker}\,f)&=\bar{f}((a*b)\mathrm{Ker}\,f)\\&=f(a*b)=f(a)\cdot(b)\\&=\bar{f}(a\,\mathrm{Ker}\,f)\cdot\bar{f}(b\,\mathrm{Ker}\,f).\end{aligned}$$

故 $\bar{f}$ 保持运算，是群同构映射。最后得到

$$G_1/\mathrm{Ker}\,f\cong f(G_1).$$

例 1 H 是群 G 的正规子群。令 $\varphi:G\to G/H$，$\varphi(a)=aH$，称 φ 为自然同态。φ 的同态核

$$\begin{aligned}\mathrm{Ker}\varphi&=\{x\mid x\in G,\ \varphi(x)=H\}\\&=\{x\mid x\in G,\ xH=H\}=H.\end{aligned}$$

例 2 令 $G_1=\langle \mathrm{Z},+\rangle$，$G_2=\langle a\rangle=\{a^0,a^1,\cdots,a^{n-1}\}$ 且 $a^n=e$。定义 $f:\mathrm{Z}\to\langle a\rangle$，$f(n)=a^n$，$f$ 是从 G_1 到 G_2 的满同态映射，它的同态核

$$\mathrm{Ker}\,f=\{m\mid m\in \mathrm{Z},\ a^m=a^0\}=\{kn\mid k\in \mathrm{Z}\}=n\mathrm{Z}.$$

由群同态基本定理知

$$\mathrm{Z}/n\mathrm{Z}\cong\langle a\rangle.$$

而 $\mathrm{Z}/n\mathrm{Z}\cong \mathrm{Z}n$，所以 $\langle a\rangle\cong \mathrm{Z}n$。我们再次得到“$n$ 阶循环群同构于模 n 同余类群”这个结论。

例 3 用同态基本定理证明定理 6.7 中的 4°。

证明 已知 H_2 是 $f(G_1)$ 的正规子群。定义 $\bar{f}:G_1\to f(G_1)/H_2$。$\bar{f}(a)=f(a)H_2$。由于 $f:G_1\to f(G_1)$ 是满同态映射，易知 $\bar{f}$ 也是满同态映射。

$$\operatorname{Ker}\tilde{f} = \{x \mid x \in G_1,\ f(x)H_2 = H_2\}$$
$$= \{x \mid x \in G_1,\ f(x) \in H_2\} = f^{-1}(H_2),$$

由定理 6.6 知 $f^{-1}(H_2)$ 是 G_1 的正规子群。再由群同态基本定理知

$$G_1/f^{-1}(H_2) \cong f(G_1)/H_2.$$

定理 6.10 H, K **均是群** G **的正规子群，且** $K \subseteq H$，**那么**

$$G/H \cong \frac{G/K}{H/K}.$$

证明 K 是群 G 的子群。K 对于 G 中的运算构成群。$K \subseteq H$，H 对于 G 中的运算也构成群. 从而 K 也是 H 的子群。任取 $h \in H \subseteq G$，$k \in K$，由于 K 是 G 的正规子群，$h' * k * h \in K$，所以 K 是 H 的正规子群，从而 H/K 是群。

令 $f: G/K \to G/H$，$f(aK) = aH$，容易证明 f 与代表元选取无关，f 是映射，并且是满射。

$$f(aK \cdot bK) = f(a * bK) = a * bH = aH \cdot bH$$
$$= f(aK) \cdot f(bK),$$

f 是满同态映射。它的同态核

$$\operatorname{Ker} f = \{aK \mid aK \in G/K,\ f(aK) = H\}$$
$$= \{aK \mid aK \in G/K,\ aH = H\}$$
$$= \{aK \mid a \in H\} = H/K.$$

由同态基本定理知

$$\frac{G/K}{H/K} \cong G/H.$$

证毕。

习 题

1. H 是交换群 G 的子群，证明 H 的每个左陪集也是一个右陪集.
2. H 是 G 的子群，a, b 是 G 中的元素，证明以下六个命题是等价的。

(1) $a' * b \in H$.　(2) $b' * a \in H$.　(3) $b \in aH$.

(4) $a \in bH$.　(5) $aH = bH$.　(6) $aH \cap bH \neq \varnothing$.

3. 写出 A_4 关于 $H=\{e,(12)(34),(13)(24),(14)(23)\}$ 的左陪集分解与右陪集分解.

4. H 是群 G 的指数为 2 的子群. 证明：对于 G 的任意元素 a 必有 $a^2\in H$，若 H 的指数为 3，是否对 G 的任意元素 a 有 $a^3\in H$? 证明你的断言.

5. H,K 是 G 的两个子群，$[G:H]=m$，$[G:K]=n$，证明子群 $H\cap K$ 在 G 中的指数 $\leqslant m\cdot n$.

6. 群 G 的阶数为 $p\cdot q$，其中 p,q 均为素数且 $p<q$. 证明:群 G 不可能有两个不同的 q 阶子群.

7. H 是 G 的正规子群. 如果 a 和 b 属于 H 的同一个陪集中，c 和 d 属于 H 的同一个陪集中，那么 $a*c$ 和 $b*d$ 属于 H 的同一个陪集中.

8. G 是整数加群，$H=\{mk|k\in \mathbf{Z}\}$. 商群 G/H 含有哪些元素? 它的单位元是什么? 写出该商群的乘法表.

9. 如果群 G 只含有一个某阶子群，那么该子群必是正规子群.

10. H_1 和 H_2 是 G 的正规子群. 证明：$H_1\cap H_2$，$H_1\cdot H_2$ 也是 G 的正规子群.

11. H_1，H_2，N 都是 G 的正规子群，并且 $H_1\subset H_2$，证明 $H_1\cdot N$ 是 $H_2\cdot N$ 的正规子群.

12. H,K 都是群 G 的正规子群并且 $H\cap K=\{e\}$. 证明：对任意 $h\in H$，$k\in K$，都有 $h*k=k*h$.

13. 在 $G=\{f|f:\mathbf{Z}\to \mathbf{Z}/(2)\}$ 上定义运算"+".

$$(f+g)(x)=f(x)+g(x).$$

证明：$\langle G,+\rangle$ 是交换群，并且非零元素的阶为 2.

14. 在非零实数乘法群中，如下定义的映射 f 中，哪些是同态映射，并且找出它的同态核.

(1) $f_1(x)=|x|$.　　(2) $f_2(x)=2x$.　　(3) $f_3(x)=x^2$.

(4) $f_4(x)=\dfrac{1}{x}$.　　(5) $f_5(x)=-x$.　　(6) $f_6(x)=-\dfrac{1}{x}$.

15. 令 $G=\{A|A\in(\mathbf{Q})_n,\ |A|\neq 0\}$，$G$ 对于矩阵乘法构成群. $f:G\to \mathbf{R}^*$，$f(A)=|A|$. 证明：f 是从群 G 到非零实数乘群 $\mathbf{R}^*$ 的同态映射. 求 $f(G)$ 和 $\mathrm{Ker}\,f$.

16. G 是交换群，k 是取定的正整数. $f:G\to G$，$f(a)=a^k$. 证明：f 是同态映射. 求出 $f(G)$ 和 $\mathrm{Ker}\,f$.

17. $G=\langle a\rangle$ 是 n 阶循环群，$G'=\langle b\rangle$ 是 m 阶环循群. 证明

$$m|nk \Leftrightarrow \exists\varphi:G\to G' \text{是同态映射并且 } \varphi(a)=b^k.$$

18. H 是 G 的正规子群，$[G:H]=m$. 证明：对于 G 的任意元素 x，$x^m\in H$.

19. H,K 是 G 的正规子群. 如果 G/H，G/K 是交换群，那么 $G/H\cap K$ 也是交换群.

20. 在群 G 中，a、b 是 G 中的元素，称 $a'*b'*a*b$ 为 G 的换位元. 证明：

(1) G 的所有有限个换位元乘积构成 G', G' 是 G 的正规子群.

(2) G/G' 是交换群.

(3) 若 N 是 G 的正规子群且 G/N 是交换群，那么 G' 是 N 的子群.

7 环 和 域

实数或复数系统包含两个基本的二元运算：加法和乘法。在群论中仅仅处理一个二元运算，更没有涉及两个二元运算的关系——乘法对加法的分配律。本章将依照这类系统建立一种新的代数结构——环和域。

7.1 环 的 定 义

定义 7.1 在具有两个二元运算 + 和 · 的集合 R 中，如果

1° $\langle R, +\rangle$ 是交换群，

2° $\langle R, \cdot\rangle$ 是带 1 半群，

3° 乘法对加法的左右分配律，即对任意 $a, b, c\in R$，

$$(b+c)\cdot a=b\cdot a+c\cdot a,$$

$$a\cdot(b+c)=a\cdot b+a\cdot c,$$

则称 $\langle R, +, \cdot\rangle$ 为环。

如果环 $\langle R, +, \cdot\rangle$ 中，对任意 $a, b\in R$，$a\cdot b=b\cdot a$，则称该环是交换环。

从环的定义中我们看到环中的两个运算 + 和 · 的地位是不相同的。集合 R 对于 + 构成交换群，而对于 · 只是构成带 1 半群。R 中的元素不一定有乘法逆元。是于有乘法逆元的元素称为环中的可逆元。

下面先看几个例子。

例 1 $\langle \mathrm{R}, +, \cdot\rangle$，$\langle \mathrm{C}, +, \cdot\rangle$，$\langle \mathrm{Q}, +, \cdot\rangle$ 分别为实数环，复数环和有理数环，其中 + 与 · 运算就是普通的加法和乘法运算。它们统称为数环。

例 2 全体 n 阶整数方阵 $(Z)_n$ 对于矩阵加法和乘法构成 n 阶矩阵环 $\langle (Z)_n, +, \cdot \rangle$。全部元素为 0 的 n 阶方阵为零元，n 阶单位矩阵为乘法单位元。该环是非交换环。

例 3 $\langle G, + \rangle$ 是交换群。$E = \{f \mid f: G \to G$ 是同态映射$\}$。在 E 上定义二元运算 $+$ 和 $\cdot$：$f, g \in E$，对任意 $x \in G$，

$$(f+g)(x) = f(x) + g(x),$$

$$(f \cdot g)(x) = f(g(x)).$$

证明 $\langle E, +, \cdot \rangle$ 是环。它称为交换群 G 上的自同态环。

证明 对于 $f, g \in E$，$\forall x \in G$，定义 $(f+g)(x) = f(x) + g(x)$。显然 $f+g$ 是 G 上的映射。由于 f, g 都是 G 上的自同态映抛，

$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y) \\ &= (f(x)+f(y)) + (g(x)+g(y)) \\ &= (f(x)+g(x)) + (f(y)+g(y)) \\ &= (f+g)(x) + (f+g)(y).\end{aligned}$$

$f+g$ 保持加法运算，所以 $f+g$ 是 G 上的自同态映射，即 $f+g \in E$。由于 $\langle G, + \rangle$ 是交换群，所以 E 中的 $+$ 运算满足结合律和交换律。令 $f_0: G \to G$，$\forall x \in G$，$f_0(x) = O_G$，其中 O_G 是交换群 $\langle G, + \rangle$ 的零元。f_0 是 E 的零元。对于 $f_y: G \to G$，定义 $f_{-y}: G \to G$，$\forall x \in G$，$f_{-y}(x) = -f_y(x)$。f_{-y} 是 f_y 的负元。综上分析知 $\langle E, + \rangle$ 是交换群。

对于 $f, g \in E$，$\forall x \in G$，定义 $(f \cdot g)(x) = f(g(x))$。显然 $f \cdot g$ 是 G 上的映射。由于 f, g 都是 G 上的自同态映射，

$$\begin{aligned}(f \cdot g)(x+y) &= f(g(x+y)) = f(g(x) + g(y)) \\ &= f(g(x)) + f(g(y)) = (f \cdot g)(x) + (f \cdot g)(y).\end{aligned}$$

$f \cdot g$ 保持加法运算，所以 $f \cdot g$ 是 G 上的自同态映射，即 $f \cdot g \in E$。映射的合成运算满足结合律。令 $f_1: G \to G$，$\forall x \in G$，$f_1(x) = x$，f_1 是 E 的乘法单位元。综上知 $\langle E, \cdot \rangle$ 是带 1 半群。

对于 $f, g, h \in E$，$\forall x \in G$，

$$(f\cdot(g+h))(x)=f((g+h)(x))=f(g(x)+h(x))$$
$$=f(g(x))+f(h(x))=(f\cdot g+f\cdot h)(x),$$
$$((g+h)\cdot f)(x)=(g+h)(f(x))=g(f(x))+h(f(x))$$
$$=(g\cdot f+h\cdot f)(x),$$
即 $f\cdot(g+h)=f\cdot g+f\cdot h$，$(g+h)\cdot f=g\cdot f+h\cdot f$，$\cdot$对 $+$ 满足左、右分配律。于是 $\langle E,+,\cdot\rangle$ 是环并且是非交换环。

例 4 在 $Z_n=\{[0],[1],\cdots,[n-1]\}$ 上定义
$$[i]+[j]=[i+j],$$
$$[i]\cdot[j]=[i\cdot j].$$
容易证明如此定义的同余类加法和乘法与代表元选取无关，即当 $[i_1]=[i_2]$，$[j_1]=[j_2]$，则 $[i_1+j_1]=[i_2+j_2]$，$[i_1\cdot j_1]=[i_2\cdot j_2]$。显然 $\langle Z_n,+\rangle$ 是交换群，其中 $[0]$ 为零元。$[-i]$ 是 $[i]$ 的负元；$\langle Z,\cdot\rangle$ 是带 1 半群，其中 $[1]$ 为单位元。此外$\cdot$对 $+$ 满足左、右分配律。所以 $\langle Z_n,+,\cdot\rangle$ 是环，并称为模 n 同余类环。

在环的定义中指出 $\langle R,+\rangle$ 是交换群，它满足左、右消去律。从 $x+a=a$，$a+x=0$，$a+b=a+c$ 分别推出 $x=0$，$x=-a$，$b=c$。这里 0 表示环 R 的零元。

定理 7.1 在环 $\langle R,+,\cdot\rangle$ 中，0 和 1 分别是零元和乘法单位元。对于 R 中元素 a，b 有

1° $a\cdot 0=0\cdot a=0$，

2° $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$，特别地 $(-1)a=-a$。

3° $(-a)\cdot(-b)=a\cdot b$，特别地 $(-1)\cdot(-1)=1$。

证明

1° $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$，由消去律得到 $a\cdot 0=0$。同理可证 $0\cdot a=0$。

2° $a\cdot(-b)+(a\cdot b)=a\cdot((-b)+b)=a\cdot 0=0$，得知 $a\cdot(-b)=-(a\cdot b)$。同理可证 $(-a)\cdot b=-(a\cdot b)$。特别地，取 $b=1$，得到 $(-1)\cdot a=-a$。

3° $(-a)(-b)=-(a\cdot(-b))=-(-(a\cdot b))=a\cdot b$。特别

地，取 $a=b=1$，得到 $(-1)(-1)=1$。

证毕。

在环 $\langle R,+,\cdot\rangle$ 中，如果零元 0_R 等于乘法单位元 1_R，即 $0_R=1_R$，任取 $r\in R$，

$$0_R=r\cdot 0_R=r\cdot 1_R=r,$$

即 $R=\{0_R\}$。

定义 7.2 在环 $\langle R,+,\cdot\rangle$ 中，$|R|=1$，那么 $R=\{0_R\}$，称该环为平凡环。

如果 $|R|\neq 1$，那么必有 $0_R\neq 1_R$，称该环为非平凡环。

例 5 环 R 中所有可逆元构成群。

证明 $\langle R,+,\cdot\rangle$ 是环，令

$$H=\{r\mid r\in R,\ \exists r'\in R,\ r\cdot r'=r'\cdot r=1_R\}.$$

任取 $r_1, r_2\in H$，存在 $r_1', r_2'\in R$ 使得 $r_1\cdot r_1'=r_1'\cdot r_1=1_R$，$r\cdot r_2'=r_2'\cdot r_1=1_R$。由于 $(r_1\cdot r_2)\cdot(r_2'\cdot r_1')=(r_2'\cdot r_1')\cdot(r_1\cdot r_2)=1_R$。知 $r_2'\cdot r_1'\in R$ 是 $r_1\cdot r_2$ 的逆元。故 $r_1\cdot r_2\in H$，即 H 对$\cdot$运算是封闭的。因 $\langle R,\cdot\rangle$ 是带 1 半群，$H\subseteq R$。显然运算 $\cdot$ 在 H 中也满足结合律。由 $1_R'=1_R, 1_R\in H$。任意 $r\in H$。r 是 r' 的逆元。故 $r'\in H$。综合分析知 $\langle H,\cdot\rangle$ 是群。

7.2 整环和域

本节介绍两个特殊的环——整环和域，我们先观察两个例子。

在整数环 $\langle Z,+,\cdot\rangle$ 中，0 是零元。对任何 $m, n\in Z$，如果 $m\cdot n=0$，则必有 $m=0$ 或 $n=0$。换句话说，如果 $m\neq 0$，$m\cdot n=0$，则必有 $n=0$。这个性质允许我们在等号两边消去非零元素。这是因为如果 $ab=ac$ 且 $a\neq 0$，那么 $a\cdot(b-c)=0$。由此推出 $b-c=0$，即 $b=c$。在模 4 同余类环中，[0]是零元。$[2]\neq[0]$，但是 $[2]\cdot[2]=0$。从 $[2]\cdot[1]=[2]\cdot[3]$ 推不出 $[1]=[3]$。

定义 7.3 在环 $\langle R,+,\cdot\rangle$ 中，对于非零元素 $a\in R$，如果存在一个非零元素 $b\in R$ 使得 $a\cdot b=0$，则称 a 为左零因子。如果存在一个非零元素 $b\in R$ 使得 $b\cdot a=0$，则称 a 为右零因子。若 a 既是左零因子又是右零因子，则称 a 为零因子。

定理 7.2 环 $\langle R,+,\cdot\rangle$ 中没有左零因子当且仅当环中乘法有左右消去律。

证明 如果环 $\langle R,+,\cdot\rangle$ 中没有左零因子，对于 R 中的非零元素 a，有 $a\cdot b=a\cdot c$，即 $a\cdot(b-c)=0$，推出 $b-c=0$，即 $b=c$。故左消去律成立。

假若该环中有右零子 $b\in R$，且 $b\neq 0$，那么必然存在非零元素 c 使得 $c\cdot b=0$。这样 c 就是 R 的左零因子，与环 R 中无左零因子矛盾。换句话说，在环 R 中无左零因子，那么也一定没有右零因子。用上面同样方法可以证明右消去律成立。

反过来，环 R 中成立乘法的左右消去律。任取环 R 中的非零元素 a，如果 $a\cdot b=0$，由于 $a\cdot b=0=a\cdot 0$，用左消去律得到 $b=0$，那么 a 不是左零因子。由 a 的任意性知，环 R 中无左零因子。证毕。

定义 7.4 非平凡交换环 $\langle R,+,\cdot\rangle$ 中，如果没有零因子，则称之为整环。

显然在整环中。对于 R 中元素 a，b，若 $a\cdot b=0$，则必有 $a=0$ 或 $b=0$。根据定理 7.2 知，整环中有左、右消去律。

定理 7.3 在整环中，每个非零元素的加阶或者是无限的，或者是素数。

证明 先研究环 R 的乘法单位元 1_R 的加阶。如果 1_R 的加阶是无限的，假设 R 的某个非零元素 a 的加阶为 m，即 $ma=0_R$。

$$ma=\underbrace{a+a+\cdots+a}_{m}=(1_R+1_R+\cdots+1_R)\cdot a=0_R.$$

由于 $a\neq 0_R$，得出 $m\cdot 1_R=\underbrace{1_R+1_R+\cdots+1_R}_{m}=0_R$。这与 1_R 的阶是

无限的矛盾，故不可。所以 R 中的所有非零元素的加阶必是无限的。如果 1_R 的加阶为 k，假设 $k=m\cdot n$，即 $(m\cdot n)1_R=0_R$，而 $(m\cdot n)1_R=(m\cdot 1_R)\cdot(n\cdot 1_R)$，且 R 是整环，推出 $m\cdot 1_R=0_R$ 或 $n\cdot 1_R=0_R$。这与 1_R 的加阶为 $m\cdot n$ 矛盾，故不可。从而 1_R 的加阶必是素数。现令 1_R 的加阶为素数 p，任取 R 中的非零元素 a，

$$p\cdot a=\underbrace{a+a+\cdots+a}_{p}=a\cdot(\underbrace{1_R+1_R+\cdots+1_R}_{p})=a\cdot 0_R=0_R.$$

由此可知元素 a 的加阶 l 是 p 的因子。而 $a\neq 0_R$，所以 a 的加阶也为素数 p。**证毕。**

定义 7.5　在整环中，如果每个非零元素的加阶为素数 p，则称该整环的特征为 p。如果每个非零元素的加阶是无限的，则称该整环的特征为 0 。

在特征为 p 的整环中，

$$(a+b)^p=a^p+c_p^1a^{p-1}b+\cdots+c_p^{p-1}ab^{p-1}+b^p,$$

由于 $p\mid c_p^i$，$1\leqslant i\leqslant p-1$，于是 $(a+b)^p=a^p+b^p$。

定义 7.6　在非平凡交换环 R 中，如果对每个非零元素 a，存在 $a'\in R$ 使得 $a\cdot a'=1_R$，则称该环为域。换句话说，非平凡交换环中，如果所有非零元素构成交换群，则该环是域。

定理 7.4　域是整环。

证明　在域 F 中，若 $a\cdot b=0$ 且 $a\neq 0$，那么 a 有逆元 a'

$$b=1\cdot b=(a'\cdot a)\cdot b=a'\cdot(a\cdot b)=a'\cdot 0=0.$$

这就是说 F 中没有零因子，即域 F 是整环。**证毕。**

定理 7.5　有限整环是域。

证明　$\langle R,+,\cdot\rangle$ 是有限整环，$R=\{r_0,r_1,\cdots,r_n\}$，不妨假设 $r_0=0_R$，$r_1=1_R$。任取 $r_i\in R$，$1\leqslant i\leqslant n$，

$$r_iR=\{r_i\cdot r_0,\ r_i\cdot r_1,\ \cdots,\ r_i\cdot r_n\}\subseteq R,$$

当 $k\neq l$ 时，由于整环中有左右消去律，显然 $r_i\cdot r_k\neq r_i\cdot r_l$，所以 $|r_iR|=|R|$，并推出 $r_iR=R$。存在 j 使 $r_i\cdot r_j=r_1=1_R$，即 r_j 是 r_i 的乘法逆元。这说明 R 中所有非零元素均有乘法逆元，R 是域

证毕。

从定理 7.4 和 7.3 知有限域的特征为素数 p。

例 1 p 为素数时，$\langle Z_p, +, \cdot\rangle$ 是域。

证明 $Z_p=\{[0],[1],\cdots,[p-1]\}$，$\langle Z_p, +, \cdot\rangle$是非平凡交换环。$[0]$是零元，$[1]$是乘法单位元。如果 $[a]\neq 0$ 且$[a]\cdot[b]=[0]$，那么 $[a\cdot b]=[0]$，即 $p|a\cdot b$。而 $a\nmid p$。推出 $b|p$，即$[b]=[0]$。这些说明 $\langle Z_p, +, \cdot\rangle$是有限整环，从而它是域。

例 2 $\langle\{a+b\sqrt{2}\,|a, b\in Q\}, +, \cdot\rangle$ 是域。

证明 令 $Q(\sqrt{2})=\{a+b\sqrt{2}\,|a, b\in Q\}$。不难验证 $\langle Q(\sqrt{2}), +\rangle$是交换群，$\langle Q(\sqrt{2}), \cdot\rangle$ 是带 1 半群。$0+0\sqrt{2}$ 是零元，$-a-b\sqrt{2}$ 是 $a+b\sqrt{2}$的负元。$1+0\sqrt{2}$是乘法单位元。乘法是可交换的并且乘法与加法有左、右分配律。当$a+b\sqrt{2}\neq 0$时，$\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in Q(\sqrt{2})$ 是 $a+b\sqrt{2}$ 的乘法逆元。所以 $\langle Q(\sqrt{2}), +, \cdot\rangle$ 是域。

7.3 子环和环同态

定义 7.7 在环 $\langle R, +, \cdot\rangle$ 中，S 是 R 的非空子集。如果

1° $\langle S, +\rangle$ 是 $\langle R, +\rangle$的子群。

2° S 对乘法 · 运算封闭。

3° 环 R 的乘法单位元 $1_R\in S$。

则称 $\langle S, +, \cdot\rangle$ 是 $\langle R, +, \cdot\rangle$ 的子环。

显然如此定义的子环 $\langle S, +, \cdot\rangle$ 本身是环。

例 1 $\langle Z, +, \cdot\rangle$ 是 $\langle Q, +, \cdot\rangle$ 的子环。

例 2 $\langle R, +, \cdot\rangle$ 是环。令

$$Z(R)=\{x|x\in R, \forall a\in R, ax=xa\},$$

则 $\langle Z(R), +, \cdot\rangle$ 是 $\langle R, +, \cdot\rangle$ 的子环。

证明 $Z(R)$ 是 R 中与所有元素可交换的元素组成的集

合。由于 R 的乘法单位元 $1_R \in Z(R)$，$Z(R)$ 是 R 的非空子集。任取 $x, y \in Z(R)$，$\forall a \in R$，

$$(x+y)\cdot a = x\cdot a + y\cdot a = a\cdot x + a\cdot y = a\cdot(x+y),$$

$$(-x)\cdot a = -xa = -ax = a\cdot(-x),$$

故 $\langle Z(R), +\rangle$ 是 $\langle R, +\rangle$ 的子群。又任取 $x\cdot y \in Z(R)$，$\forall a \in R$，

$$(x\cdot y)\cdot a = x\cdot(y\cdot a) = x\cdot(a\cdot y) = (x\cdot a)\cdot y$$

$$= (a\cdot x)\cdot y = a\cdot(x\cdot y),$$

$x\cdot y \in Z(R)$，即在 $Z(R)$ 中乘法运算 · 是封闭的。综上知 $\langle Z(R), +, \cdot\rangle$ 是 $\langle R, +, \cdot\rangle$ 的子环。

定义 7.8 R_1 和 R_2 是环，f 是从 R_1 到 R_2 的映射。1_{R_1} 和 1_{R_2} 分别是 R_1 和 R_2 的乘法单位元。$\forall a, b \in R_1$。

$$f(a+b) = f(a) + f(b),$$

$$f(a\cdot b) = f(a)\cdot f(b),$$

$$f(1_{R_1}) = 1_{R_2},$$

那么称 f 是从 R_1 到 R_2 的环同态映射。

如果 f 是满射(单射，双射)，则称 f 为满环同态映射(单一环同态映射，环同构映射)。

例 3 从 R^n 到其自身的线性变换全体对加法和乘法运算构成环 $\langle L(\mathrm{R}^n, \mathrm{R}^n), +, \cdot\rangle$。$n$ 阶实数矩阵环记为 $\langle M(n\times n, \mathrm{R}), +, \cdot\rangle$. 证明这两个环是同构的。

证明 从 R^n 到其自身的线性变换对于 R^n 的一组基 $x_1, x_2, \cdots, x_n$ 有

$$\alpha\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{pmatrix}.$$

我们定义 $f: L(\mathrm{R}^n, \mathrm{R}^n) \to M(n\times n, \mathrm{R})$，

$$f(\alpha)=\begin{pmatrix} a_{11}\ a_{12}\cdots a_{1n} \\ a_{21}\ a_{22}\cdots a_{2n} \\ \cdots \\ a_{n1}\ a_{n2}\cdots a_{nn} \end{pmatrix}.$$

在线性代数中学过：在一组基之下，每个线性变换对应一个 $n\times n$ 矩阵，并且线性变换的和对应于矩阵的和，线性变换的积对应于矩阵的乘积。所以，对于线性变换 $\alpha,\ \beta\in L(\mathrm{R}^n,\mathrm{R}^n)$，

$$f(\alpha+\beta)=f(\alpha)+f(\beta).$$

$$f(\alpha\cdot\beta)=f(\alpha)\cdot f(\beta).$$

若 γ 是单位线性变换，则 $f(\gamma)$ 是单位矩阵。反过来，对任意 n 阶实数矩阵都可以定义相应的线性变换。不同的线性变换对应不同的矩阵，所以 f 是满射和单射，从而 f 是环同构映射。$\langle L(\mathrm{R}^n,\mathrm{R}^n),\ +,\ \cdot\rangle$ 与 $\langle M(n\times n,\ \mathrm{R}),\ +,\ \cdot\rangle$ 是同构的。

例 4 $\langle \mathrm{Z}_{24},\ +,\ \cdot\rangle$ 与 $\langle \mathrm{Z}_4,\ +,\ \cdot\rangle$ 是两个环。令 $f:\mathrm{Z}_{24}\to\mathrm{Z}_4$，$f([x]_{24})=[x]_4$。首先指出映射 f 的定义与代表元选取无关。这是因为若 $[x]_{24}=[y]_{24}$，那么 $24\mid(x-y)$。而 $4\mid 24$，故 $4\mid(x-y)$，即 $[x]_4=[y]_4$。

$$\begin{aligned} f([x]_{24}+[y]_{24})&=f([x+y]_{24})=[x+y]_4\\ &=[x]_4+[y]_4=f([x]_{24})+f([y]_{24}).\\ f([x]_{24})\cdot[y]_{24})&=f([x\cdot y]_{24})=[x\cdot y]_4\\ &=[x]_4\cdot[y]_4=f([x]_{24})\cdot f([y]_{24}). \end{aligned}$$

$f([1]_{24})=[1]_4$.

所以 f 是环同态映射。

环同态映射也有类似于群同态映射的一些性质。

定理 7.7 **f 是从环 R_1 到环 R_2 的同态映射，O_{R_1} 和 O_{R_2} 分别是环 R_1 和 R_2 的零元，**

1° $f(O_{R_1})=O_{R_2}$.

2° $f(-a)=-f(a)$.

3° **若 a 是 R_1 的可逆元，则 $f(a)$ 是 R_2 的可逆元并且**

$f(a')=(f(a))'$.

证明 f 是从环 R_1 到环 R_2 的同态映射，那么 f 也是从交换群 $\langle R, +\rangle$ 到交换群 $\langle R_2, +\rangle$ 的群同态映射．所以 1° 与 2° 显然成立。若 a 是 R_1 的可逆元。即存在 $a' \in R_1$ 使 $a \cdot a' = a' \cdot a = 1_{R_1}$，那么

$$f(a)\cdot f(a') = f(a \cdot a') = f(1_{R_1}) = 1_{R_2},$$
$$f(a')\cdot f(a) = f(a' \cdot a) = f(1_{R_1}) = 1_{R_2}.$$

从而 $f(a')=(f(a))'$。**证毕．**

例 5 $\langle Z, +, \cdot\rangle$ 与 $\langle Zn, +, \cdot\rangle$ 是环。令 f: $Z \to Zn$, $f(m) = [m]$，f 是满同态映射．$\langle Z, +, \cdot\rangle$ 是整环，$\langle Zn, +, \cdot\rangle$ 不一定是整环。当 $n = k \cdot l$ 时，$[k]\cdot[l]=[0]$，$[k]$，$[l] \neq [0]$，环 $\langle Zn, +, \cdot\rangle$ 中有零因子。

例 6 $\langle Z\times Z, +, \cdot\rangle$ 与 $\langle Z, +, \cdot\rangle$ 是环。令 f: $Z\times Z \to Z$, $f(a, b) = a$，f 是满同态映射．$Z\times Z$ 中的非零元素 $(2, 0)$，$(0, 1)$ 是零因子，$\langle Z\times Z, +, \cdot\rangle$ 不是整环，但 $\langle Z, +, \cdot\rangle$ 是整环。

以上两例说明环同态映射并不保持环的全部代数结构。为此给出如下定理。

定理 7.3 **f 是从环 R_1 到 R_2 的同构映射，如果 R_1 是整环(域)，那么 R_2 也是整环(域)**

证明 R_1 是整环，它是非平凡交换环且没有零因子。令 f: $R_1 \to R_2$ 是同构映射，由于 $0_{R_1} \neq 1_{R_1}$，$0_{R_2} = f(0_{R_1}) \neq f(1_{R_1}) = 1_{R_2}$，于是 R_2 是非平凡环．任取 x_2, $y_2 \in R_2$，必存在 x_1, $y_1 \in R_1$ 使 $f(x_1) = x_2$, $f(y_1) = x_2$.

$$\begin{aligned} x_2 \cdot y_2 &= f(x_1)\cdot f(y_1) = f(x_1 y_1) = f(y_1 \cdot x_1) \\ &= f(y_1)\cdot f(x_1) = y_2 \cdot x_2. \end{aligned}$$

R_2 是交换环。如果 $x_2, y_2 \in R_2$ 且 $x_2 \cdot y_2 = 0_{R_1}$，由于存在 $x_1, y_1 \in R_1$ 使 $f(x_1) = x_2$, $f(y_1) = y_2$.

$$0_{R_2} = x_2 \cdot y_2 = f(x_1)\cdot f(y_1) = f(x_1 \cdot y_1),$$

而 f 是单射，必有 $x_1 \cdot y_1 = 0_{R_1}$，因 R_1 中无零因子，推出 $x_1 = 0_{R_1}$ 或

$y_1 = 0_{R_1}$，进而得出 $x_2 = f(x_1) = 0_{R_2}$ 或 $y_2 = f(y_1) = 0_{R_2}$。这说明 R_2 中无零因子，故 R_2 是整环。

如果 R_1 是域，任取 R_2 的非零元素 x_2，因 f 是满射，必存在 $x_1 \in R_1$ 使得 $f(x_1) = x_2$。f 又是单射，x_1 是 R_1 的非零元素，它在 R_1 中有逆元 x_1'，$f(x_1') \in R_2$，

$$f(x_1) \cdot f(x_1') = f(x_1 \cdot x_1') = (f(1_{R_1}) = 1_{R_2},$$

那么 $f(x_1') \in R_2$ 是 x_2 的逆元。由 x_2 的任意性知 R_2 是域。

证毕

定理 7.9 $\langle R, +, \cdot \rangle$**是环。在非空集合** R_1 **上定义了两个运算** + **和** ·**。如果存在满射** $f: R \to R_1$，**对于所有** $a, b \in R$ **有**

$$f(a+b) = f(a) + f(b),$$

$$f(a \cdot b) = f(a) \cdot f(b),$$

那么 $\langle R_1, +, \cdot \rangle$**是环。**

证明 $f: R \to R_1$ 是满射。R_1 中元素都可以写成 $f(a)$ 形式，$a \in R$。由于 $\langle R, + \rangle$ 是交换群，所以 R_1 中 + 运算满足交换律和结合律。$f(0_R) \in R_1$ 是 R_1 的零元。$f(-a)$ 是 $f(a)$ 的负元。故 $\langle R_1, + \rangle$ 是交换群。由于 $\langle R, \cdot \rangle$ 是带 1 半群。所以 R_1 中·运算是封闭的并且满足结合律。$f(1_R) \in R_1$ 是 R_1 的乘法单位元。故 $\langle R_1, \cdot \rangle$ 是带 1 半群。由 R 中·对 + 有左、右分配律。所以 R_1 中·对 + 也有左、右分配律。

综上讨论知 $\langle R_1, +, \cdot \rangle$ 是环。

7.4 理想与商环

这一节我们将用定义商群类似的方法定义商环。这里与正规子群相对应的概念是理想。商环是由对于一个理想的陪集组成的集合。

定义 7.9 I **是环** R **的空子集。如果** $\forall x, y \in I$，$r \in R$，**有** $x - y \in I$，$x \cdot r \in I$ **并且** $r \cdot x \in I$，**则称** I **是** R **的一个理想。**

在此定义中。由于 $\forall x, y \in I$, $x-y\in I$ 推出 $\langle I, +\rangle$ 是 $\langle R, +\rangle$的子群。

对每个环 R 都有 R 和 $\{0_R\}$ 这两个理想。我们称这两个理想叫作平凡理想。非平凡理想称为真理想。

如果 I_1, I_2 是环 R 的理想。定义

$$I_1\cdot I_2=\left\{\sum_{k=1}^{n} r_{1k}\cdot r_{2k}\,\middle|\, r_{1k}\in I_1,\ r_{2k}\in I_2,\ 1\leqslant k\leqslant n,\ n=1, 2, \cdots,\right\}$$

$$I_1+I_2=\{r_1+r_2\,|\,r_1\in I_1,\ r_2\in I_2\},$$

那么 $I_1\cdot I_2$ 与 I_1+I_2 都是R的理想。证明留作习题。

例 1 在模 6 同余类环 $\langle Z_6, +, \cdot\rangle$ 中，$I_1=\{[0], [3]\}$ 是理想。在环 $\langle Z\times Z, +, \cdot\rangle$ 中，$I_2=\{(0, n)\,|\,n\in Z\}$ 是理想。

在环 R 中，利用 R 的理想 I 建立了一个关系。我们称环 R 中的元素 x 与 y 模 I 同余，当且仅当 $x-y\in R$。不难证明 R 中的模同余关系是等价关系。元素 x 所在的等价类

$$[x]=\{y\,|\,y\in R, x-y\in I\}=\{x+i\,|\,i\in I\}=x+I.$$

在商集合 R/I 中定义$[x]+[y]=[x+y]$, $[x]\cdot[y]=[x\cdot y]$。如此定义的等价类加法和乘法是与代表元选取无关的。这是因为，如果 $[x_1]=[x_2]$, $[y_1]=[y_2]$，那么由 $x_1-x_2\in I$, $y_1-y_2\in I$ 知

$$(x_1+y_1)-(x_2+y_2)=(x_1-x_2)+(y_1-y_2)\in I,$$

$$x_1\cdot y_1-x_2\cdot y_2=x_1\cdot(y_1-y_2)+(x_1-x_2)\cdot y_2\in I.$$

故 $(x_1+y_1)+I=(x_2+y_2)+I$, $x_1\cdot y_1+I=x_2\cdot y_2+I$。

定理 7.10 **I 是环 R 的理想。$R/I=\{x+I\,|\,x\in R\}$ 中的加法 $+$ 和乘法 $\cdot$ 如上定义。$\langle R/I, +, \cdot\rangle$ 为环，并称为 R 模 I 的商环。**

证明 R/I 中的 $+$ 和 $\cdot$ 运算是由等价类代表元的 $+$ 与 $\cdot$ 运算实现的。$\langle R/I, +\rangle$中 $+$ 运算满足结合律和交换律。0_R+I 是 R/I 的零元。$(-x)+I$ 是 $x+I$ 的负元。故$\langle R/I, +\rangle$是交换群。$\langle R/I, \cdot\rangle$中$\cdot$运算满足结合律，$1_R+I$ 是其单位元，故$\langle R/I, \cdot\rangle$是带 1 半群。$\cdot$对 $+$ 显然有左、右分配律。综上知 $\langle R/I, +, \cdot\rangle$是

环。证毕。

例 2 在例 1 中

$$Z_6/I_1=\{[0]+I_1,\ [1]+I_1,\ [2]+I_1\},$$

$$Z\times Z/I_2=\{(m,\ 0)+I\,|\,m\in Z\}.$$

如果环 R 的理想 I 中有 R 的可逆元 r，$r'\subset R$。由理想的定义知 $r'\cdot r=1_R\in I$。任取 $\tilde{r}\in R$，$\tilde{r}\cdot 1_R=\tilde{r}\subset I$，于是 $R\subseteq I$。又知理想 I 是 R 的非空子集 $I\subseteq R$，故得出 $I=R$，即该理想必是平凡理想。

在域 F 中，若 I 是 F 的理想且 $I\neq\{0_F\}$，则必存在一个非零元素 $a\in I$。而域中所有非零元素都有逆，所以必定 $I=F$。这就是说域 F 只有两个理想 $\{0_F\}$ 和 F，F 没有真理想。从而域 F 的商域或是 $F/\{0_F\}=\{r+\{0_F\}\,|\,r\in F\}\cong F$，或是 $F/F=\{F\}\cong\{0_F\}$。它们的结构过于简单，没有必要深入讨论。

下面我们来讨论一种特殊的理想。

定理 7.11 **R 是交换环，对于 R 中元素 a，$(a)=\{a\cdot r\,|\,r\in R\}$ 是 R 的一个理想，称它为由 a 生成的理想。这类特殊的理想叫作主理想。**

证明 对于 R 中元素 a，$a\cdot 1_R=a$，显然 $a\in(a)$。如果 a_1，$a_2\in(a)$，即存在 r_1，$r_2\in R$ 使 $a_1=a\cdot r_1$，$a_2=a\cdot r_2$，而 $a_1-a_2=a\cdot(r_1-r_2)$，故 $a_1-a_2\in(a)$。又对任意 $r\in R$，$r\cdot a_1=r\cdot(a\cdot r_1)=a\cdot(r\cdot r_1)\in(a)$，$a_1\cdot r=a\cdot(r_1\cdot r)\in(a)$。所以 (a) 是 R 的理想。**证毕。**

把这个思想推广到交换环 R 的子集上。令 $S=\{r_1,\ r_2,\ \cdots,\ r_k\}\subseteq R$。

$(r_1,\ r_2,\ \cdots,\ r_k)=\{r_1\cdot a_1+r_2\cdot a_2+\cdots+r_k\cdot a_k\,|\,a_1,a_2,\cdots,a_k\in R\}$。

是 R 的理想，并称它为 S 生成的理想。

定义 7.10 **如果环 R 的所有理想都是主理想，则称 R 是主理想环。**

例 3 证明 $\langle Z,\ +,\ \cdot\rangle$ 是主理想环。

证明 设 I 是整数环 $\langle Z, +, \cdot\rangle$ 的理想。如果 I 中没有非零元素，即 $I=\{0\}$，那么 I 是由 0 生成的理想。如果 I 中有非零元素，不妨假设有一个正整数 $a\in I$（假若 $b<0$，且 $b\in I$。因为 I 是理想，$-1\in Z$，$-b=(-1)\cdot b\in I$，并且 $-b>0$）。这样就可以在 I 中找到一个最小的正整数 k。对于 I 中任意元素 n，$n=mk+l$，其中 $0\leqslant l<k$。由于 I 是理想，推出 $l=n-mk\in I$。而 k 是 I 中最小的正整数，得知必有 $l=0$，即 $n=mk\in(k)$。从而 $I\subseteq(k)$。又由于 $k\in I$ 显然 $mk\in I$，故 $(k)\subseteq I$。最后得知 $I=(k)$。这说明整数环是主理想环。

7.5 多项式环

7.5.1 环上的多项式

环 $\langle R, +, \cdot\rangle$ 上的多项式定义为

$$P(x)=a_0+a_1\cdot x+\cdots+a_n\cdot x^n,\ a_n\neq 0_R,\ n\geqslant 0,$$

其中 $a_0, a_1, \cdots, a_n\in R$ 称为系数，x 为未定元，n 为 $p(x)$ 的次数，即 $\deg(p(x))=n$。环 R 上的非零元素称为零次多项式（或常数多项式），零元素 0_R 称为零多项式。

环 R 上的全体多项式组成的集合 $R[x]$，在其上定义运算 + 和·，$f(x), g(x)\in R[x]$。其中 $f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{j=0}^{m}b_j\cdot x^j$，

$$f(x)+g(x)=\sum_{k=0}^{\max(m,n)}(a_k+b_k)\cdot x^k.$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}c_k\cdot x^k,\quad c_k=\sum_{i+j=k}a_i\cdot b_j,\ 0\leqslant k\leqslant m+n.$$

其中若 $m>n$ 时 $a_k=0$，$n<k\leqslant m$；若 $m<n$ 时，$b_k=0$，$m<k\leqslant n$。不难验证 $\langle R[x], +, \cdot\rangle$ 是环。零多项式是零元，$-f(x)$ 是 $f(x)$ 的负元。常数多项式 1_R 是乘法单位元。

如若 R 是整环，即 R 是非平凡交换环并且没有零因子，$f(x)$ 与 $g(x)$ 是 $R[x]$ 中的非零多项式。它们的次数分别为 $n, m(\geq 0)$，即 $f(x)=a_nx^n+\cdots$，$g(x)=b_mx^m+\cdots$，a_n，$b_m \neq O_R$。由于 R 是整环，$a_n \cdot b_m \neq O_R$。而

$$f(x)\cdot g(x)=a_nb_mx^{n+m}+\cdots$$

是非零多项式，从而 $R[x]$ 中无零因子。又 $R[x]$ 是非平凡交换环，故 $R[x]$ 是整环。

7.5.2 域上的多项式

定理 7.13 **F 是域，$f(x)$，$g(x)$ 是多项式环 $F[x]$ 的元素。如果 $g(x)$ 不是零多项式，则存在唯一的，$g(x)$，$r(x) \in F(x)$，使得**

$$f(x)=q(x)\cdot g(x)+r(x)\text{。}$$

其中 $r(x)$ 或是零多项式或是次数小于 $\deg g(x)$ 的多项式。

证明 令 $g(x)=b_0+b_1x+\cdots+b_mx^m$，$b_m \neq O_F$，$m \geq 0$。考虑集合。

$$S'=\{f(x)-S(x)\cdot g(x)\,|\,S(x)\in F[x]\}$$

有两种可能的情况：

1° 零多项式 $O_F \in S'$。此时存在 $q(x)\in F[x]$，使得 $f(x)=q(x)\cdot g(x)$。

2° 零多项式 $O_F \notin S'$。记 S' 中次数最小的多项式为 $r(x)$，存在 $q(x)\in F[x]$，使 $r(x)=f(x)-q(x)\cdot g(x)$，即 $f(x)=q(x)\cdot g(x)+r(x)$。假设 $r(x)=c_tx^t+\cdots+c_0$，$c_t \neq 0_F$，$t \geq m$，现构造一个新的多项式

$$\begin{aligned} r_1(x)&=f(x)-q(x)\cdot g(x)-c_t\cdot b_m'x^{t-m}\cdot g(x)\\ &=r(x)-c_tx^t+\cdots, \end{aligned}$$

于是 $\deg(r_1(x))<\deg(r(x))$，而

$$r_1(x)=f(x)-[q(x)+c_t\cdot b_m'x^{t-m}]\cdot g(x)\in S'\text{。}$$

这就与 $r(x)$ 是 S' 中次数最低的多项式相矛盾。故不可。所以必

有 $\deg(r(x))<\deg(g(x))$。

下面证明 $q(x)$，$r(x)$ 是唯一的。现假设 $q_1(x)$，$r_1(x)$ 及 $q_2(x)$，$r_2(x)$ 均满足

$$f(x)=q_1(x)\cdot g(x)+r_1(x),$$
$$f(x)\neq q_2(x)\cdot g(x)+r_2(x),$$

并且 $r_1(x)$，$r_2(x)$ 的次数均小于 $g(x)$ 的次数 $(=m)$。将上面两式相减得到

$$(q_1(x)-q_2(x))\cdot g(x)=r_2(x)-r_1(x).$$

如果 $q_1(x)-q_2(x)$ 不是零多项式，那么等式左边多项式次数大于等于 m，而等式右边多项式次数小于 m，产生矛盾，故不可。所以必有 $q_1(x)=q_2(x)$。由此又推出 $r_1(x)=r_2(x)$。证毕。

这个定理说明域上的多项式可以作除法。其商和余式是唯一确定的。如果 $f(x)=q(x)\cdot g(x)$，则称 $g(x)$ 是 $f(x)$ 的因式。特别地，取 $g(x)=x-a$，$f(x)$ 除以 $x-a$ 的余式是域 F 的元素，即

$$f(x)=q(x)\cdot(x-a)+r_0,\quad r_0\in F.$$

令 $x=a$，得到 $r_0=f(a)$。由此可知，在 $F[x]$ 中多项式 $x-a$ 是 $f(x)$ 的因式当且仅当 $f(a)=0_F$，这时称 a 是多项式 $f(x)$ 的根。

定理 7.14　域 F 上的多项式环 $F[x]$ 是主理想环。

证明　设 I 是 $F[x]$ 的一个理想。若 I 中没有非零多项式，则 $I=\{0_F\}$，它是由 0_F 生成的理想。若 I 中有非零多项式，其中次数最低的非零多项式记为 $g(x)$。对于 $g(x)$ 有两种可能的情况。

1°　$\deg(g(x))=0$，即 $g(x)=a\in F$ 且 $a\neq 0_F$。a 在 F 中有逆 a'，$a'\in F[x]$。$a'\cdot a=1_F\in I$。故 $I=F[x]$，它是由 1_F 生成的理想。

2°　若 $\deg(g(x))\neq 0$，任取 $f(x)\in I$，由定理 7.13 知存在 $q(x)$，$r(x)\in F[x]$ 使 $f(x)=q(x)\cdot g(x)+r(x)$。因为 $g(x)\in I$，且 I 是 $F[x]$ 的理想，推出 $r(x)\in I$。由于 $g(x)$ 是 I 中次数最低的多项式，故必有 $r(x)=0_F$，即 $f(x)=q(x)\cdot g(x)\in(g(x))$。由 $f(x)$ 的任意性知 $I\subseteq(g(x))$。反过来，$g(x)\in I$，对任何 $g(x)\in$

$F[x]$。$q(x)\cdot g(x)\in I$。从而$(g(x))\subseteq I$。综上分析知$I=(g(x))$。

所以域F上的多项式环$F[x]$是主理想环。

7.5.3 域上的多项式商环

域F的多项式环$F[x]$是主理想环。$F[x]$的理想都是$P=(P(x))$形式，其中$P(x)=a_0+a_1x+\cdots+a_nx^n$，$a_n\neq 0_F$，那么

$$F[x]/P=\{f(x)+P\mid f(x)\in F[x]\}.$$

而$f(x)=q(x)\cdot p(x)+r(x)$，$f(x)-r(x)\in(p(x))$，即$f(x)+P=r(x)+P$。所以

$$F[x]/P=\{b_0+b_1x+\cdots+b_{n-1}x^{n-1}+P\mid b_0,b_1,\cdots,b_{n-1}\in F\}.$$

例 1 写出$Z_2[x]/(x^2+x+1)$，的加法表和乘法表。

解 $Z_2=\{[0],[1]\}$，我们简写成$Z_2=\{0,1\}$。(x^2+x+1)是$Z_2[x]$的主理想。令$P=(x^2+x+1)$，

$$\begin{aligned}Z_2[x]/P&=\{(ax+b)+P\mid a,b\in Z_2\}\\&=\{P,1+P,x+P,1+x+P\}.\end{aligned}$$

它的加法表和乘法表为：

+	P	$1+P$	$x+P$	$1+x+P$
P	P	$1+P$	$x+P$	$1+x+P$
$1+P$	$1+P$	P	$1+x+P$	$x+P$
$x+P$	$x+P$	$1+x+P$	P	$1+P$
$1+x+P$	$1+x+P$	$x+P$	$1+P$	P

$\cdot$	P	$1+P$	$x+P$	$1+x+P$
P	P	P	P	P
$1+P$	P	$1+P$	$x+P$	$1+x+P$
$x+P$	P	$x+P$	$1+x+P$	$1+P$
$1+x+P$	P	$1+x+P$	$1+P$	$x+P$

7.6 环同态定理

定义 7.11 φ **是从环** R_1 **到环** R_2 **的同态映射。** 0_{R_2} **是** R_2 **的零元，** $\mathrm{Ker}\ \varphi=\{r \mid r\in R_1,\ \varphi(r)=0_{R_2}\}$**。称为** φ **的同态核。**

定理 7.15 φ **是从** R_1 **到** R_2 **的环同态映射，** $\mathrm{Ker}\ \varphi$ **是** R_2 **的理想。**

证明 φ 是从 R_1 到 R_2 的环同态映射，φ 也是从交换群 $\langle R_1, +\rangle$ 到 $\langle R_2, +\rangle$ 的群同态映射。由定理 6.6 知 $\mathrm{Ker}\ \varphi$ 是 $\langle R_1, +\rangle$ 的正规子群，任取 $x_1, x_2\in \mathrm{Ker}\ \varphi$，$x_1-x_2\in \mathrm{Ker}\ \varphi$。又若 $x\in \mathrm{Ker}\varphi$，$r\in R_1$，

$$\varphi(x\cdot r)=\varphi(x)\cdot\varphi(r)=0_{R_1}\cdot\varphi(r)=0_{R_2},$$

知 $x\cdot r\in \mathrm{Ker}\ \varphi$。同理可证 $r\cdot x\in \mathrm{Ker}\ \varphi$。从而 $\mathrm{Ker}\ \varphi$ 是 R_1 的理想。**证毕。**

定理 7.16 （环同态基本定理）

环 R_1 **的任意商环都是环** R_1 **的同态象。若** φ **是从环** R_1 **到** R_2 **的满同态映射。那么**

$$R_1/\mathrm{Ker}\ \varphi\cong R_2.$$

证明 设 I_1 是环 R_1 的理想。令 $\tilde{\varphi}$：$R_1\to R_1/I_1$，$\tilde{\varphi}(r)=r+I_1$，显然 $\tilde{\varphi}$ 是满射。又对任意 $r_1, r_2\in R_1$，

$$\begin{aligned}\tilde{\varphi}(r_1+r_2)&=(r_1+r_2)+I=(r_1+I)+(r_2+I)\\&=\tilde{\varphi}(r_1)+\tilde{\varphi}(r_2),\\\tilde{\varphi}(r_1\cdot r_2)&=(r_1\cdot r_2)+I=(r_1+I)\cdot(r_2+I)\\&=\tilde{\varphi}(r_1)\cdot\tilde{\varphi}(r_2),\\\tilde{\varphi}(1_{R_1})&=1_{R_1}+I,\end{aligned}$$

知 $\tilde{\varphi}$ 是满同态映射，$\tilde{\varphi}(R_1)=R_1/I_1$。

若 φ 是从环 R_1 到 R_2 的满同态映射，那么 φ 也是从 $\langle R_1, +\rangle$ 到 $\langle R_2, +\rangle$ 的群同态映射。从群同态基本定理知 φ：$R_1\mathrm{Ker}\ \varphi\to R_2$，$\varphi(r+\mathrm{Ker}\ \varphi)=\varphi(r)$ 是群同构映射。又

$$\varphi((r_1+\mathrm{Ker}\,\varphi)\cdot(r_2+\mathrm{Ker}\,\varphi))=\varphi(r_1\cdot r_2+\mathrm{Ker}\,\varphi)$$
$$=\varphi(r_1\cdot r_2)=\varphi(r_1)\cdot\varphi(r_2)$$
$$=\varphi(r_1+\mathrm{Ker}\,\varphi)\cdot\varphi(r_2+\mathrm{Ker}\,\varphi)。$$
$$\varphi(1_{R_1}+\mathrm{Ker}\,\varphi)=\varphi(1_{R_1})=1_{R_2}$$

知 φ 是环同构映射，从而

$$R_1/\mathrm{Ker}\,\varphi\cong R_2$$

证毕。

例 1 Q[x] 是有理数域 Q 上的多项式全体。令 $Q(\sqrt{2})=\{a+b\sqrt{2}\,|a,\ b\in\mathrm{Q}\}$。证明

$$\mathrm{Q}[x]/(x^2-2)\cong Q(\sqrt{2})。$$

证明 令 ψ: Q[x]→$Q(\sqrt{2})$，$\psi(f(x))=f(\sqrt{2})$ 是环同态映射。任取 $a+b\sqrt{2}\in Q(\sqrt{2})$，$a+bx\in\mathrm{Q}[x]$。$\psi(a+bx)=a+b\sqrt{2}$。所以 ψ 是满同态映射。下面求 Ker ψ。若 $p(x)\in\mathrm{Ker}\,\psi$，即 $p(\sqrt{2})=0$。取 $g(x)=x^2-2$，由定理 7.13 知

$$p(x)=q(x)(x^2-2)+a_0+a_1x,\ a_0,\ a_1\in\mathrm{Q}。$$

由 $p(\sqrt{2})=0$ 推出 $a_0+a_1\sqrt{2}=0$，得知必有 $a_0=a_1=0$。并由此得到 $p(-\sqrt{2})=a_0-a_1\sqrt{2}=0$，于是 x^2-2 是 $p(x)$ 的因式，Ker $\psi=(x^2-2)$。根据环同态基本定理知

$$\mathrm{Q}[x]/(x^2-2)\cong Q(\sqrt{2})。$$

例 2 证明 R[x]/$(x^2+1)\cong$ C。

证明 令 ψ: R[x]→C，$\psi(f(x))=f(i)$ 是环同态映射。任取 $a+bi\in$ C，$a+bx\in$ R[x]，使得 $\psi(a+bx)=a+bi$，故 ψ 是满同态映射。

任取 $p(x)\in\mathrm{Ker}\,\psi$，即 $p(i)=0$。取 $g(x)=x^2+1$。由定理 7.13 知

$$p(x)=q(x)(x^2+1)+a_0+a_1x,\ a_0,\ a_1\in\mathrm{R}。$$

由 $p(i)=a_0-a_1i=0$ 推出 $a_0=a_1=0$。并由此得到 $p(-i)=0$。于是 x^2+1 是 $p(x)$ 的因式。Ker $\psi=(x^2+1)$。再根据环同态基本定理知

$$\mathbf{R}[x]/(x^2+1)\cong \mathbf{C}.$$

定理 7.17 f 是从 R_1 到 R_2 的环同态映射.

1° S_1 是 R_1 的子环, 则 $f(S_1)$ 是 R_1 的子环. 特别地, $f(R_1)$ 是 R_2 的子环.

2° S_1 是 R_1 的理想, 则 $f(S_1)$ 是 $f(R_1)$ 的理想.

3° S_2 是 $f(R_1)$ 的子环, 则 $f^{-1}(S_2)$ 是 R_1 的子环.

4° S_2 是 $f(R_1)$ 的理想, 则 $f^{-1}(S_2)$ 是 R_1 的理想. 且 $R_1/f^{-1}(S_2)\simeq f(R_1)/S_2$.

证明 这里只证明 1° 和 4°.

1° f 是从 R_1 到 R_2 的环同态映射. 那么 f 是从 $\langle R_1, +\rangle$ 到 $\langle R_2\ +\rangle$ 的群态态映射. S_1 是 R_1 的子环, 那么 $\langle S_1, +\rangle$ 是 $\langle R_1, +\rangle$ 的子群, 由定理 6.7 知 $\langle f(S_1), +\rangle$ 是 $\langle R_2, +\rangle$ 的子群. 任取 $x_2, y_2\in f(S_1)$, 存在 $x_1, y_1\in S_1$ 使得 $f(x_1)=x_2$, $f(y_1)=y_2$. 因 $x_1\cdot y_1\in S_1$, 所以

$$x_2\cdot y_2=f(x_1)\cdot f(y_1)=f(x_1\cdot y_1)\in f(S_1).$$

$f(S_1)$ 对乘法 $\cdot$ 是封闭的. 又 $1_{R_1}\in S_1$, $f(1_{R_1})=1_{R_2}$, 即 $1_{R_2}\in f(S_1)$. 由此看出 $\langle f(S_1), +, \cdot\rangle$ 是 $\langle R_2, +, \cdot\rangle$ 的子环.

特别地, R_1 是 R_1 的子环, 所以 $f(R_1)$ 是 R_2 的子环.

4° 已知 S_2 是 $f(R_1)$ 的理想, $f(R_1)/S_2$ 是环. 令 $\psi: f(R_1)\to f(R_1)/S_2$, $\psi(f(r_1))=f(r_1)+S_2$. 显然 ψ 是满射. 又因 f 从 R_1 到 $f(R_1)$ 的满射, 所以 $\psi\cdot f$ 是从 R_1 到 $f(R_1)/S_2$ 的满射. 对于 $r_1, r_2\in R_1$,

$$\begin{aligned}(\psi\cdot f)(r_1+r_2)&=\psi(f(r_1+r_2))=f(r_1+r_2)+S_2\\&=(f(r_1)+f(r_2))+S_2\\&=(f(r_1)+S_2)+(f(r_2)+S_2)\\&=(\psi\cdot f)(r_1)+(\psi\cdot f)(r_2),\\(\psi\cdot f)(r_1\cdot r_2)&=\psi(f(r_1\cdot r_2))=f(r_1\cdot r_2)+S_2\\&=(f(r_1)\cdot f(r_2))+S_2\\&=(f(r_1)+S_2)\cdot(f(r_1)+S_2)\end{aligned}$$

$$=(\psi\cdot f)(r_1)\cdot(\psi\cdot f)(r_2),$$

$$(\psi\cdot f)(1_{R_1})=\psi(f(1_{R_1}))=f(1_{R_1})+S_2=1_{R_2}+S_2.$$

从而 $\psi\cdot f$ 是满同态映射。

$$\mathrm{Ker}(\psi\cdot f)=\{r\mid r\in R_1,\ \psi\cdot f(r)=S_2\}$$

$$=\{r\mid r\in R_1,\ f(r)\in S_2\}=f^{-1}(S_2).$$

由环同态基本定理知

$$R_1/f^{-1}(S_2)\cong f(R_1)/S_2.$$

定理 7.18 I_1，I_2 **是环** R **的两个理想**，$I_2\subseteq I_1$，**则** I_1/I_2 **是** R/I_2 **的理想且**

$$\frac{R/I_2}{I_1/I_2}\cong R/I_1.$$

证明 I_1，I_2 是环 R 的理想，$I_2\subseteq I_1\subseteq R$。我们建立商集合 $I_1/I_2=\{i+I_2\mid i\in I_1\}\subseteq R/I_2$。定义 f：$R/I_2\to R/I_1$，$f(r+I_2)=r+I_1$。当 $r_1+I_2=r_2+I_2$ 时，$r_1-r_2\in I_2$，而 $I_2\subseteq I_1$，所以 $r_1-r_2\in I_1$，从而 $r_1+I_1=r_2+I_1$。该映射与代表元选取无关。f 是满射。对于 r_1，$r_2\in R$，

$$f((r_1+I_2)+(r_2+I_2))=f((r_1+r_2)+I_2)=(r_1+r_2)+I_1$$

$$=(r_1+I_1)+(r_2+I_1)$$

$$=f(r_1+I_2)+f(r_2+I_2),$$

$$f((r_1+I_2)\cdot(r_2+I_2))=f(r_1\cdot r_2+I_2)=r_1\cdot r_2+I_1$$

$$=(r_1+I_1)\cdot(r_2+I_1)$$

$$=f(r_1+I_2)\cdot f(r_2+I_2),$$

$$f(1_R+I_2)=1_R+I_1,$$

f 是满同态映射。

$$\mathrm{Ker}\ f=\{r+I_2\mid r+I_1=I_1\}=\{r+I_2\mid r\in I_1\}=I_1/I_2.$$

由环同态基本定理知

$$\frac{R/I_2}{I_1/I_2}\cong R/I_1.$$

7.7 素理想和极大理想

I 是环 R 的理想，则 R/I 是环．什么样的理想能使 R/I 为整环或者为域呢？先看个例子．我们已经讲过整数环 $\langle Z, +, \cdot\rangle$ 中所有理想都是主理想．p 为素数，$(p)=\{k\cdot p \mid k\in Z\}$ 是 Z 的理想．

$$Z/(p)=\{(p), 1+(p), \cdots, (p-1)+(p)\}\cong Z_p.$$

如果 $(i+(p))\cdot(j+(p))=(p)$，即 $i\cdot j\in(p)$，$p\mid i\cdot j$，那么推出 $p\mid i$ 或 $p\mid j$，即 $i+(p)=(p)$ 或 $j+(p)=(p)$．$Z/(p)$ 为整环．由此引出素理想的概念．

定义 7.12 **I 是非平凡交换环 R 的理想，$I\neq R$．对于 R 的任意元素 a, b，如果 $a, b\in I$ 能推出 $a\in I$ 或 $b\in I$，那么称 I 为) 的素理想．**

定理 7.19 **I 是非平凡交换环 R 的理想．R/I 是整环当且仅当 I 是素理想．**

证明 R/I 是整环．R 的任意元素 a，b，如果 $a\cdot b\in I$，即 $(a+I)\cdot(b+I)=a\cdot b+I=I$，由于 R/I 中没有零因子．所以必有 $a+I=I$ 或者 $b+I=I$（I 是 R/I 的零元）．于是 $a\in I$ 或者 $b\in I$．所以 I 是素理想．

反过来，如果 I 是 R 的素理想．在环 R/I 中，若 $(a+I)\cdot(b+I)=a\cdot b+I=I$，必有 $a\cdot b\in I$．因 I 是素理想．推出或者 $a\in I$，或者 $b\in I$，即 $a+I=I$ 或者 $b+I=I$．这说明 R/I 中没有零因子．所以 R/I 是整环．

例 1 域 F 上的多项式环 $F[x]$ 是主理想环，(x)是素理想．

证明 (x) 是 $F(x)$ 的理想，商环

$$\begin{aligned}F[x]/(x)&=\{f(x)+(x)\mid f(x)\in F[x]\}\\&=\{a+(x)\mid a\in F\}.\end{aligned}$$

定义 φ：$F[x]/(x)\to F$，$\varphi(a+(x))=a$ 是环同构映射．$F[x]/$

$\langle x\rangle\cong F$，所以 $F[x]/(x)$ 是整环. 由定理 7.19 知 (x) 是素理想。

定义 7.13 I **是环** R **的理想，**$I\neq R$**. 若** $I\subset M$**，**M **是** R **的理想，则必有** $M=R$**. 我们称** I **是** R **的极大理想.**

例 2 整数环 Z 中，p 是素数，(p) 是 Z 的素理想，它也是 Z 的极大理想. 这是因为，若 M 是 Z 的理想并且 $(p)\subset M$. M 中必有元素 $m\notin(p)$，即 $m=kp+l$，$0<l<p$. l 与 p 互素，那么存在 $a, b\in Z$ 使 $la+pb=1$，由 m，$p\in M$，推出 $l\in M$，进而得知 $1\in M$. 最后得出 $M=Z$.

例 4 域上的多项式环 $F[x]$ 中，(x) 是 $F[x]$ 的素理想. 它也是 $F[x]$ 的极大理想. 这是因为如果 M 是 $F[x]$ 的理想而且 $(x)\subset M$. 那么存在 $f(x)=a_nx^n+\cdots+a_1x+a_0\in M$，$a_0\neq 0$. $f(x)\notin(x)$. 令 $f(x)=f_1(x)+a_0$，$f_1(x)\in(x)\subset M$，推出 $a_0\in M$. a_0 是域 F 的非零元素，它是可逆元. $F[x]$的理想 M 包含可逆元 a_0 则必有 $M=F[x]$.

定理 7.20 I **是非平凡交换环** R **的理想.**R/I **是域当且仅当** I **是** R **的极大理想。**

证明 已知 R/I 是域，$I\neq R$. 若 $I\subset M$，M 是 R 的理想，那么存在 $a\in M$ 且 $a\notin I$. 显然 $a+I$ 是域 R/I 的非零元素，它的逆元是 $x+I$，即 $(a+I)\cdot(x+I)=1+I$. 因 $a\in M$，$x\in R$，M 是 R 的理想，有 $a\cdot x\in M$. 又 $I\subset M$，故 $1+I=a\cdot x+I\subseteq M$. 由此推出 $1\in M$. 从而 $M=R$. 这就证明了 I 是极大理想.

反过来，I 是极大理想，$a\notin I$，$a+I$ 是 R/I 的非零元. 如果 $x+I$ 是 $a+I$ 的逆，x 应满足

$$(a+I)(x+I)=a\cdot x+I=1_R+I,$$

即 $a\cdot x-1_R\in I$. 考虑集合

$$A=\{-i+ax\mid i\in I,\ x\in R\}.$$

显然 $I\subset A$. A 是 R 的非空子集，任取 $-i_1+ax_1$，$-i_2+ax_2\in A$，$y\in R$，

$$(-i_1+ax_1)-(-i_2+ax_2)=-(i_1-i_2)+a(x_1-x_2)\in A,$$

$$(-i_1+ax_1)\cdot y=-i_1y+a(x_1\cdot y)\in A,$$

知 A 是 R 的理想且 $I\subset A$。由于 I 是 R 的极大理想，必有 $A=R$，于是 R 的乘法单位元 $1_R\in A$。存在 $i_0\in I$，$x_0\in R$ 使 $1_R=-i_0+ax_0$，即 $ax_0-1_R\in I$，x_0+I 就是 $a+I$ 的逆元。从而 R/I 是域。

如果 I 是非平凡交换环 R 的极大理想。那么 R/I 是域。而域是整环，R/I 是整环，又推出 I 是 R 的素理想。得到如下推论

推论 7.1　非平凡交换环的极大理想一定是素理想。

此推论的逆命题不一定成立。例如整数环 Z 上的多项式环 Z[x]，(x) 是 Z[x] 的素理想。Z[x]/(x)≅Z。而 Z 不是域，故 (x) 不是 Z[x] 的极大理想。

习　题

1．下列代数系统哪些是环？

(1) ⟨Z×Z，+，·⟩，其中+与·均是对分量的运算。

(2) ⟨2Z×Z，+，·⟩，其中+与·同上。

(3) ⟨R，+，∘⟩，其中+为数加，$a\circ b=|a|\cdot b$。

2．写出下列各环的全部可逆元。

(1) ⟨Z，+，·⟩。　　(2) ⟨Q，+，·⟩。

(3) ⟨Z_4，+，·⟩。　　(4) ⟨Z_6，+，·⟩。

3．在环 ⟨R，+，·⟩ 中，如果 ⟨R，+⟩ 是循环群，则 ⟨R，+，·⟩ 是交换环。

4．在环 R 中，如果对于任意 $a\in R$ 均有 $a^2=a$，则称该环是布尔环。证明

(1) $\forall a\in R$，$2a=0$。

(2) R 是交换环。

5．下列环中哪些是整环，哪些是域？说明理由。

(1) ⟨Z×Z，+，·⟩

(2) ⟨$\{a+b\sqrt{2}\mid a,b\in Z\}$，+，·⟩

(3) ⟨$\{a+b\sqrt{3}\mid a,b\in Q\}$，+，·⟩

6．若 a 是环 R 的可逆元，则

(1) $-a$ 也是可逆元。

(2) a 不是零因子。

7．在交换环中，若 $a\cdot b$ 是零因子，则 a 是零因子或 b 是零因子。

8．E 是加群 $\langle G,+\rangle$ 的自同态环．如果 H 是 G 的子群，那么

$$E_H=\{f \mid f\in E,\ f(H)\subseteq H\}$$

是 E 的子环．

9．一个环的任意两个子环的交仍是子环．

10．令 f: $\mathrm{Z}\times\mathrm{Z}\to\mathrm{Z}$，$f(a,b)=a$．证明 f 是从环 $\langle \mathrm{Z}\times\mathrm{Z},+,\cdot\rangle$ 到环 $\langle \mathrm{Z},+,\cdot\rangle$ 的同态映射．求 $\mathrm{Ker}\,f$．

11．求出 Z_6 的全部理想．

12．若 I_1，I_2 是环 R 的理想，则 $I_1\cap I_2$，$I_1\cdot I_2$，I_1+I_2 都是 R 的理想，并且 $I_1\cdot I_2\subseteq I_1\cap I_2$。

13．证明 $I=\left\{\begin{pmatrix}0 & 2x\\ 0 & 0\end{pmatrix} \middle| x\in \mathrm{Z}\right\}$ 是 $R=\left\{\begin{pmatrix}a & b\\ 0 & c\end{pmatrix} \middle| a,b,c\in \mathrm{Z}\right\}$ 的理想．商环 R/I 是由哪些元素构成的？

14．在高斯整数环 $\mathrm{Z}[i]=\{a+bi \mid a,\ b\in \mathrm{Z}\}$ 中，$I=(2+i)$ 含有哪些元素？$\mathrm{Z}[i]/(2+i)$ 含有哪些元素？

15．令 $R=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \middle| a,b,c,d\in \mathrm{Z}\right\}$．$I=\left\{\begin{pmatrix}2m & 2n\\ 2k & 2l\end{pmatrix} \middle| m,n,k,l\in \mathrm{Z}\right\}$．证明 I 是 R 的理想．R/I 是由哪些元素组成的？

16．$\mathrm{Q}[x]$ 是有理数域 Q 上的一次多项式环，证明 $(2,x)$ 是 $\mathrm{Q}[x]$ 的主理想．

17．$F[x]$ 是数域 F 上的多项式环．在 $F[x]$ 上定义运算 $f(x)\cdot g(x)=f(g(x))$．问 $\langle F[x],+,\cdot\rangle$ 是否是环？为什么？

18．$\langle \mathrm{Z}_7,+,\cdot\rangle$ 上的多项式 $f(x)=-4+5x+3x^3$，$g(x)=3-x+4x^3$，试计算 $f(x)+g(x)$，$f(x)\cdot g(x)$．

19．域 $\langle \mathrm{Z}_2,+,\cdot\rangle$ 上的多项式 $1+x+x^2+\cdots+x^n$ 有因子 $1+x$ 当且仅当 n 为奇数。

20．找出从 Z 到 Z 的所有同态映射，并写出其同态核。

21．找出从 Z_2 到 Z 的所有同态映射。

22．证明：$(3)/(6)$ 是 $\mathrm{Z}/(6)$ 的理想，并且

$$\frac{\mathrm{Z}/(6)}{(3)/(6)}\cong \mathrm{Z}/(3).$$

23．m，r 是取定的正整数并且 $r|m$．以 $\bar{a}$ 表示 Z_m 中 a 所在的同余类，以 $[a]$ 表示在 Z_r 中 a 所在的同余类．令 f: $\mathrm{Z}_m\to\mathrm{Z}_r$，$f(\bar{a})=[a]$．证明 f 是环同态映射．求 $\mathrm{Ker}\,f$ 并找出与 $\mathrm{Z}_m/\mathrm{Ker}\,f$ 同构的环。

24．令 φ: $\mathrm{R}[x]\to R$，$\varphi(f(x))=\varphi(a_0+a_1x+\cdots+a_nx^n)=a_0$．证明 φ 是从 $R[x]$

到 R 的环满同态映射．求 $\mathrm{Ker}\,\varphi$ 并找出与 $R[x]/\mathrm{Ker}\,f$ 同构的环．

25．若 φ 是从环 R_1 到环 R_2 的满同态映射，I 是 R_1 的理想．证明

(1) $\varphi^{-1}(\varphi(I))=I+\mathrm{Ker}\,\varphi$，

(2) $\varphi(I)=R_2 \Leftrightarrow I+\mathrm{Ker}\,\varphi=R_1$．

26．整数环 Z 中，(n) 是 Z 的素理想当且仅当 $|n|=0$ 或 p，其中 p 是素数．

27．证明：在 $Z[x]$ 中，(x,n) 是极大理想当且仅当 n 为素数．

8 格与布尔代数

8.1 格的定义与性质

定义 8.1 在部分序集 $\langle A, \leqslant\rangle$ 中，如果对任意 $a, b \in A$，$\{a, b\}$ 都有一个最大下界和最小上界，则称 $\langle A, \leqslant\rangle$ 是格。

通常 $\{a, b\}$ 的最大下界称为 a 与 b 的积，记作 $a*b$；$\{a, b\}$ 的最小上界称为 a 与 b 的和，记作 $a\oplus b$。

对于 A 的任意子集，如果它有最小上界和最大下界，则它们是唯一的。在定义 8.1 中可以看出 $*$ 与 $\oplus$ 是 A 上的二元运算。格 $\langle A, \leqslant\rangle$ 有时写成 $\langle A, *, \oplus\rangle$。

不是所有的部分序集都是格。例如在图 15 中的每个部分序集都是格。

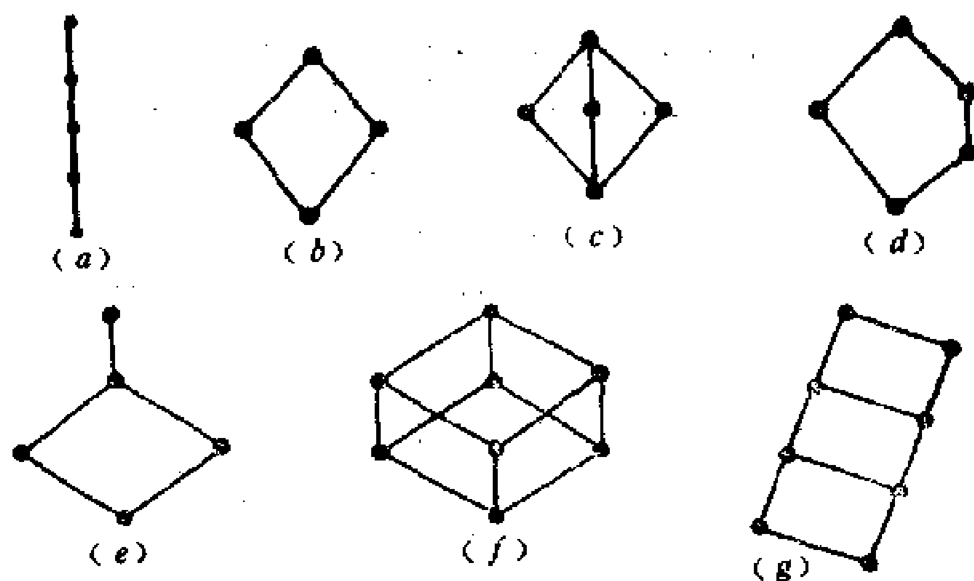


图 15

图 16 列出五个部分序集，其中，在(1)中 $\{x, y\}$ 没有上界，下界。在(2)中 $\{x, y\}$ 有最小上界，无下界。在(3) 中 $\{x, y\}$ 无上界，有最大下界。在(4)中$\{x, y\}$无上界，有下界但无最大下界。在(5)中 $\{x, y\}$有最小上界，有下界但无最大下界。所以从(1)到(5)都不是格。

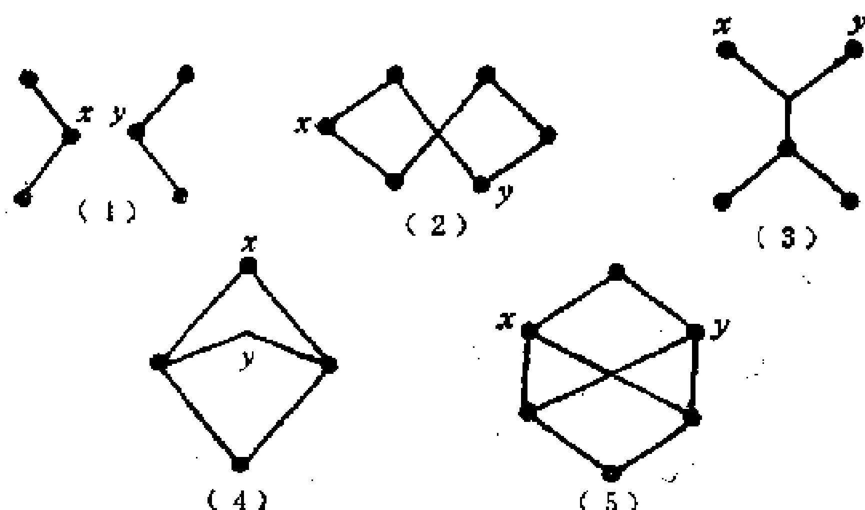


图 16

例 1 A 是集合。$\langle \mathscr{P}(A), \subseteq \rangle$ 是格。格中的运算$*$和$\oplus$分别是 $\cap$ 和 $\cup$。这是因为任取 $A_1, A_2 \in \mathscr{P}(A)$。因 $A_1 \cap A_2 \subseteq A_1$，$A_1 \cap A_2 \subseteq A_2$，故 $A_1 \cap A_2$ 是 $\{A_1, A_2\}$ 的下界。若C是$\{A_1, A_2\}$的下界，即 $C \subseteq A_1$，$C \subseteq A_2$，显然 $C \subseteq A_1 \cap A_2$。从而 $A_1 \cap A_2$ 是$\{A_1, A_2\}$ 的最大下界，即 $A_1 * A_2 = A_1 \cap A_2$。又 $A_1 \subseteq A_1 \cup A_2$，$A_2 \subseteq A_1 \cup A_2$，知 $A_1 \cup A_2$ 是 $\{A_1, A_2\}$ 的上界。若 B 是 $\{A_1, A_2\}$ 的上界，即 $A_1 \subseteq B$，$A_2 \subseteq B$，那么 $A_1 \cup A_2 \subseteq B$。从而 $A_1 \cup A_2$ 是 $\{A_1, A_2\}$ 的最小上界。即 $A_1 \oplus A_2 = A_1 \cup A_2$。

特别，当 $|A| = 2$ 时，$\langle \mathscr{P}(A), \subseteq \rangle$ 的 Hasse 图为前面的(b)。当 $|A| = 3$ 时，$\langle \mathscr{P}(A), \subseteq \rangle$ 的 Hasse 图为前面的(f)。

例 2 Z 是整数集合。$\langle Z, | \rangle$是格。格中的运算 $*$ 和$\oplus$分别是求两个数的最大公约数和最小公倍数运算。这是因为任取 a，$b \in Z$，a 与 b 的最大公约数 (a, b)满足 $(a, b)|a$，$(a, b)|b$，故

(a, b)是 $\{a, b\}$的下界。若 c 是 a 与 b 的下界，即 $c|a$, $c|b$，在第二章推论 2.1 中已指出必有 $c|(a, b)$。则 (a, b)是$\{a, b\}$ 的最大下界，即 $a*b=(a, b)$。又 a 与 b 的最小公倍数 $[a, b]$ 满足，$a|[a, b]$, $b|[a, b]$，故$[a, b]$是$\{a, b\}$的上界。若 c 是 $\{a, b\}$ 的上界，即 $a|c$, $b|c$，在第二章定理 2.4 已证明必有 $[a, b]|c$。则 $[a, b]$是 $\{a, b\}$的最小上界，即 $a\oplus b=[a, b]$。

在前面的图(b)是格 $\langle\{1, 2, 3, 6\}, |\rangle$ 的 Hasse 图，图(g)是 $\langle\{1, 2, 3, 4, 6, 8, 12, 24\}, |\rangle$ 的 Hasse 图。图 (f) 是 $\langle\{1, 2, 3, 5, 6, 10, 15, 30\}, |\rangle$ 的 Hasse 图。

例 3 设 G 是群，$L(G)=\{H|H\leqslant G\}$。$\langle L(G), \subseteq\rangle$ 是部分序集，任取$A, B\in L(G)$，A 与 B 均是 G 的子群，$A\cap B$ 也是 G 的子群。用例 1 中同样方法可以证明 $A\cap B$ 是$\{A, B\}$ 的最大下界，故 $A*B=A\cap B$。由于 A, B 是 G 的子群，显然 $A=\langle A\rangle\subseteq\langle A\cup B\rangle=\langle A, B\rangle$，$B=\langle B\rangle\subseteq\langle A\cup B\rangle=\langle A, B\rangle$。由于 $\langle A, B\rangle$ 是由 $A\cup B$ 所生成的群，$\langle A, B\rangle\subseteq G$，所以 $\langle A, B\rangle$ 是 G 的子群，即 $\langle A, B\rangle\in L(G)$。从而 $\langle A, B\rangle$ 是 $\{A, B\}$ 的上界。若 C 是 G 的子群且 $A\subseteq C$, $B\subseteq C$，那么 $A\cup B\subseteq C$。而 $\langle A, B\rangle$是包含 $A\cup B$ 的最小的群。所以 $\langle A, B\rangle\subseteq C$。这说明 $\langle A, B\rangle$是 $\{A, B\}$ 的最小上界，即 $A\oplus B=\langle A, B\rangle$。综上可知 $\langle L(G), \subseteq\rangle$ 是格，我们称它为子群格。

例 4 设 G 是群。$N(G)=\{H|H\lhd G\}$。$\langle N(G), \subseteq\rangle$ 是部分序集。任取 $A, B\in N(G)$，A 与 B 均是 G 的正规子群。$A\cap B$ 也是 G 的正规子群。故用例 1 中同样方法可以证明 $A\cap B$ 是$\{A, B\}$ 的最大下界，即 $A*B=A\cap B$。又 A, B 是 G 的正规子群，不难证明 AB 也是 G 的正规子群，并且 $\langle A, B\rangle=AB$。用例 2 中同样方法可以证明 $\langle A, B\rangle$ 是 $\{A, B\}$ 的最小上界，即 $A\oplus B=AB$。所以 $\langle N(G), \subseteq\rangle$ 是格，我们称它为正规子群格。

下面我们来研究格的性质。

定理 8.1 设 $\langle A, \leqslant\rangle$ 是格，集合 A 中的任意元素 a, b, c

满足

1° $a*a=a$，$a\oplus a=a$。 （幂等律）

2° $a*b=b*a$，$a\oplus b=b\oplus a$。 （交换律）

3° $a*(b*c)=(a*b)*c$，$a\oplus(b\oplus c)=(a\oplus b)\oplus c$。 （结合律）

4° $a*(a\oplus b)=a$，$a\oplus(a*b)=a$。 （吸收律）

证明 这里只证明1°，3°。2°和4°留作习题。

1° $\langle A,\leqslant\rangle$是格，$\leqslant$是$A$上的部分序关系。由$\leqslant$的自反性知对任意$a\in A$均有$a\leqslant a$。$a$是$\{a,a\}$的下界。若$x$是$\{a,a\}$的下界，即$x\leqslant a$，那么$a$是$\{a,a\}$的最大下界，$a*a=a$。同理可证$a\oplus a=a$。

3° 令$d=a*(b*c)$，$d'=(a*b)*c$，d是$\{a,b*c\}$的最大下界，知$d\leqslant a$，$d\leqslant b*c$。又d是$\{b,c\}$的下界，$d\leqslant b$，$d\leqslant c$。由$d\leqslant a$，$d\leqslant b$，知$d\leqslant a*b$。又由$d\leqslant a*b$，$d\leqslant c$，知$d\leqslant(a*b)*c=d'$。同理可证$d'\leqslant d$。由于部分序关系的反对称性得出$d=d'$，即$a*(b*c)=(a*b)*c$。

同理可证$a\oplus(b\oplus c)=(a\oplus b)\oplus c$。

证毕

定理8.2 $\langle A,\leqslant\rangle$**是格。对于$A$中的任意元素$a$，$b$，以下三个命题是等价的。**

1° $a\leqslant b$，

2° $a*b=a$，

3° $a\oplus b=b$。

证明

1°⇒2°，已知$a\leqslant b$，由$\leqslant$的自反性知$a\leqslant a$，那么a是$\{a,b\}$的下界。而$a*b$是$\{a,b\}$的最大下界，所以$a\leqslant a*b$。另一方面，从$a*b$的定义知$a*b\leqslant a$。由部分序关系$\leqslant$的反对称性知$a*b=a$。

2°⇒3° 已知$a*b=a$。由定理7.1中的诸性质知$b=b\oplus(b*a)=b\oplus(a*b)=b\oplus a=a\oplus b$，即$a\oplus b=b$。

$3^\circ \Rightarrow 1^\circ$　已知 $a \oplus b = b$，从 $a \oplus b$ 的定义知 b 是 $\{a, b\}$ 的最小上界。所以 $a \leqslant b$。

以上证明了三个命题的等价性。**证毕。**

定理 8.3　$\langle A, \leqslant \rangle$ **是格。对于** A **中的任意元素** a, b, c，**如果** $b \leqslant c$，**则** $a * b \leqslant a * c$，$a \oplus b \leqslant a \oplus c$。

证明　由定理 8.2 知 $b \leqslant c$ 等价于 $b * c = b$，在格中 $*$ 运算满足幂等律、结合律和交换律，

$$(a * b) * (a * c) = (a * a) * (b * c) = a * (b * c) = a * b。$$

再由定理 8.2 知 $a * b \leqslant a * c$。

同理可证 $a \oplus b \leqslant a \oplus c$。**证毕**

定理 8.4　$\langle A, \leqslant \rangle$ **是格。对于** A **中的任意元素** a, b, c **满足如下分配不等式**

$$a \oplus (b * c) \leqslant (a \oplus b) * (a \oplus c),$$

$$a * (b \oplus c) \geqslant (a * b) \oplus (a * c)。$$

证明　由 $\oplus$ 的定义知 $a \leqslant a \oplus b$，$a \leqslant a \oplus c$。再由 $*$ 的定义得到 $a \leqslant (a \oplus b) * (a \oplus c)$。又因为

$$b * c \leqslant b \leqslant a \oplus b,$$

$$b * c \leqslant c \leqslant a \oplus c,$$

及 $*$ 的定义得到 $b * c \leqslant (a \oplus b) * (a \oplus c)$。这说明 $(a \oplus b) * (a \oplus c)$ 是 $\{a, b * c\}$ 的上界，而 $a \oplus (b * c)$ 是 $\{a, b * c\}$ 的最小上界，于是

$$a \oplus (b * c) \leqslant (a \oplus b) * (a \oplus c)。$$

同理可证另一个分配不等式。**证毕**

定理 8.5　$\langle A, \leqslant \rangle$ **是格，对于** A **中任意元素** a, b, c，

$$a \leqslant b \Longleftrightarrow a \oplus (b * c) \leqslant b * (a \oplus c)。$$

证明　已知 $a \leqslant b$。在定理 8.5 的分配不等式 $a \oplus (b * c) \leqslant (a \oplus b) * (a \oplus c)$ 中代入与 $a \leqslant b$ 等价的命题 $a \oplus b = b$。得到 $a \oplus (b * c) \leqslant b * (a \oplus c)$。

反过来，已知 $a \oplus (b * c) \leqslant b * (a \oplus c)$，由于

$$a \leqslant a \oplus (b * c),$$

$$b*(a\oplus c)\leqslant b,$$

再由部分序关系$\leqslant$的传递性知$a\leqslant b$。**证毕。**

定理8.6 **$\langle A,\leqslant\rangle$是格，$A$的任意有限子集$S$均有最大下界和最小上界。**

证明 我们对A的有限子集S中的元素个数归纳证明。当$|S|=2$时，$\langle A,\leqslant\rangle$是格，对任意二元子集$\{a,b\}$均有最大下界和最小上界。故命题成立。假设$|S|=n-1$时命题成立。当$|S|=n$时，不妨令$S=\{a_1,a_2,\cdots,a_{n-1},a_n\}$，$S'=\{a_1,a_2,\cdots,a_{n-1}\}$，$|S'|=n-1$。由归纳假设它有最小上界$b'$。因为$\langle A,\leqslant\rangle$是格，$\{b',a_n\}$有最小上界$b$，即$b'\leqslant b$，$a_n\leqslant b$。而$a_i\leqslant b'$，$i=1,2,\cdots,n-1$，所以$b$是$S$的上界。若$c$也是$S$的上界，$a_i\leqslant c$，$1\leqslant i\leqslant n$，那么$c$是$S'$的上界，而$b'$是$S'$的最小上界，故$b'\leqslant c$。又$a_n\leqslant c$，$b$是$\{a_n,b'\}$的最小上界，故$b\leqslant c$。这说明$b$是$S$的最小上界。

用类似的方法可以证明S有最大下界。**证毕。**

在本定理证明中给出了一种求A的有限子集最小上界和最大下界的方法。这种证明叫做构造性证明。

$\langle A,\leqslant\rangle$是部分序集。在集合$A$上定义一个新的关系$\leqslant_1$，对于$a,b\in A$，

$$a\leqslant_1 b\Longleftrightarrow b\leqslant a.$$

显然$\langle A,\leqslant_1\rangle$也是部分序集。$\langle A,\leqslant_1\rangle$的Hasse图是把$\langle A,\leqslant\rangle$的Hasse图上下颠倒过来。$A$的二元子集$\{a,b\}$在$\langle A,\leqslant_1\rangle$中的最大下界和最小上界分别是在$\langle A,\leqslant\rangle$中的最小上界和最大下界。如果$\langle A,\leqslant\rangle$是格，那么$\langle A,\leqslant_1\rangle$也是格。前者的二元运算为$*$和$\oplus$，后者的二元运算为$*'$和$\oplus'$。在$\langle A,\leqslant\rangle$中的命题

$$a\leqslant b\Longleftrightarrow a\oplus b=b$$

在$\langle A,\leqslant_1\rangle$中写成

$$a\leqslant_1 b\Longleftrightarrow a\oplus' b=b.$$

我们把它翻译成$\langle A,\leqslant\rangle$中的语言则是

$$a\geqslant b\Longleftrightarrow a*b=b.$$

从这个例子，我们看出如下的对偶原理：一个在所有格中都成立的命题，我们把其中的 $\geqslant, \leqslant, *, \oplus$ 分别改成 $\leqslant, \geqslant, \oplus, *$ 得到该命题的对偶命题，那么对偶命题在所有格中也都成立。

例如，分配不等式 $a\oplus(b*c)\leqslant(a\oplus b)*(a\oplus c)$ 的对偶命题是分配不等式 $a*(b\oplus c)\geqslant(a*b)\oplus(a*c)$。

8.2 几种特殊的格

8.2.1 完全格和有界格

定义 8.2 如果在格 $\langle A, \leqslant\rangle$ 中，对于 A 的任意子集均有最大下界和最小上界，则称该格是完全格。

显然，当 A 是有限集合时，定理 8.6 说明格 $\langle A, \leqslant\rangle$ 是完全格。

定义 8.3 在格 $\langle A, \leqslant\rangle$ 中，若存在最大元和最小元，分别记为 1 和 0，那么 A 中任意元素 a 都满足 $0\leqslant a\leqslant 1$。我们称该格是有界格，并写成 $\langle A, \leqslant, 0, 1\rangle$。

完全格必是有界格。

在有界格中，对于 A 的任意元素 a，

$$a\oplus 0=a,\quad a*0=0,$$

$$a\oplus 1=1,\quad a*1=a.$$

在有界格中，可以用下述方式引进一个元素的补的概念。

定义 8.4 在有界格 $\langle A, \leqslant, 0, 1\rangle$ 中，对于 A 中元素 a, b，如果 $a*b=0$，$a\oplus b=1$，则称 a 是 b 的补（ b 也是 a 的补）。

一般地，在有界格中，一个元素可能没有补元，也可能有多个补元。例如图 17 中的左图里 a_1, a_2, a_3 都没有补元，右图里 a_1, a_2, a_3 互为补元。

在有界格中，最大元 1 是最小元 0 的唯一补元，最小元 0 是最大元 1 的唯一补元。这是因为 1 是有界格 $\langle A, \leqslant, 0, 1\rangle$ 的最

大元，对于 A 的任意元素 a，$a\oplus 1=1$，$a*1=a$。特别取 $a=0$，$0\oplus 1=1$，$0*1=0$。所以 0 与 1 是互补的。又若 $b\in A$ 是 0 的补元，即 $0\oplus b=1$。而 0 是最小元，$0\leqslant b$，$0\oplus b=b$。从而 $b=1$。1 是 0 的唯一补元。

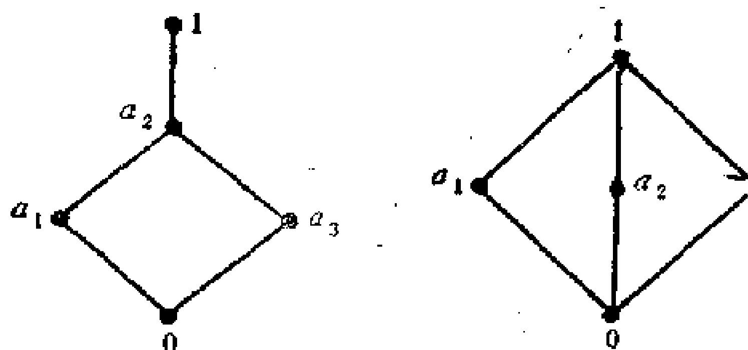


图 17

8.2.2 有 补 格

定义 8.5　在有界格 $\langle A, \leqslant, 0, 1\rangle$ 中，如果每个元素都至少有一个补元素，则称该格有补格。

例 1　$L=\{0, 1\}$。在集合 L^3 上定义关系 $\leqslant_3$。对任意 a_1，a_2，a_3，b_1，b_2，$b_3\in L$，

$$(a_1, a_2, a_3)\leqslant_3(b_1, b_2, b_3)\Longleftrightarrow a_1\leqslant b_1, a_2\leqslant b_2, a_3\leqslant b_3.$$

$\langle L^3, \leqslant_3\rangle$ 是有序数组格，其最小元和最大元分别为 $(0, 0, 0)$ 和 $(1, 1, 1)$。L^3 中元素 (a_1, a_2, a_3) 的补元为 (b_1, b_2, b_3)，其中

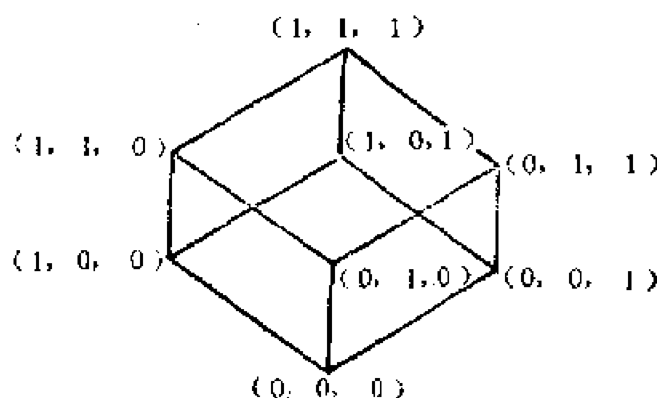


图 18

$$b_i=\begin{cases}1, & a_i=0,\\ 0, & a_i=1,\end{cases}\quad 1\leqslant i\leqslant 3.$$

$\langle L^3, \leqslant_3\rangle$ 是有补格。它的 Hasse 图为图 18。

例 2 A 是集合，$\langle\mathscr{P}(A), \subseteq\rangle$ 是有界格，其最小元和最大元分别是 ϕ 和 A。$\mathscr{P}(A)$的任意元素 B 的补元是 $A-B$。$\langle\mathscr{P}(A), \subseteq\rangle$ 是有补格。

8.2.3 分配格

定义 8.6 在格 $\langle A, \leqslant\rangle$ 中，如果对于 A 的任意元素 a, b, c 有

$$a*(b\oplus c)=(a*b)\oplus(a*c),$$

$$a\oplus(b*c)=(a\oplus b)*(a\oplus c),$$

则称 $\langle A, \leqslant\rangle$ 为分配格。

例 1 A 是集合，$\langle\mathscr{P}(A), \subseteq\rangle$ 中的二元运算$*$和$\oplus$分别为集合的交$\cap$和并$\cup$。而集合的交和并运算满足分配律，故$\langle\mathscr{P}(A), \subseteq\rangle$ 是分配格。

例 2 Z^+ 是正整数集合，$\langle Z^+, |\rangle$ 中的二元运算$*$和$\oplus$分别是求最大公因子和最小公倍数运算，它们满足分配律，故$\langle Z^+, |\rangle$ 是分配格。

例 3 图 19 中的左图是有补格，但不是分配格。这是因为

$$a_1*(a_2\oplus a_3)=a_1*1=a_1,$$

$$(a_1*a_2)\oplus(a_1*a_3)=0\oplus 0=0,$$

不满足分配等式 $a_1*(a_2\oplus a_3)=(a_1*a_2)\oplus(a_1*a_3)$。

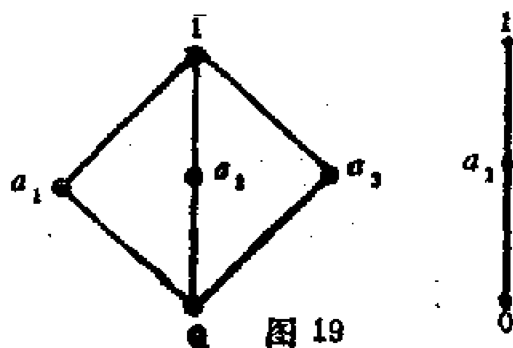


图 19

图 19 中的右图是有界分配格，但 a_1 无补元。所以有补格不一定是分配格，分配格也不一定是有补格。

定理 8.7　任意线性序集都是一个分配格。

证明　$\langle A, \leqslant\rangle$是线性序集，$A$ 中任意两个元素 a, b，或者 $a\leqslant b$，或者 $b\leqslant a$。所以

$$a*b=\begin{cases}a, & \text{如果 } a\leqslant b,\\ b, & \text{如果 } b\leqslant a.\end{cases}$$

$$a\oplus b=\begin{cases}b, & \text{如果} a\leqslant b,\\ a, & \text{如果} b\leqslant a.\end{cases}$$

$\langle A, \leqslant\rangle$ 是格。A 中任取三个元素 a, b, c，它们之间的关系可能有两种情况。

1° $a\geqslant b$ 且 $a\geqslant c$。

a 是 $\{b, c\}$的上界，$b\oplus c\leqslant a$，于是 $a*(b\oplus c)=b\oplus c$，又由 $a\geqslant b$，$a\geqslant c$，知 $a*b=b$，$a*c=c$，所以$(a*b)\oplus(a*c)=b\oplus c$。从而 $a*(b\oplus c)=(a*b)\oplus(a*c)$。

2° $a\leqslant b$ 或 $a\leqslant c$。

a 是$\{b, c\}$ 的下界，$a\leqslant b*c\leqslant b\oplus c$，于是$a*(b\oplus c)=a$。又因 $a\leqslant b$ 或 $a\leqslant c$，即 $a*b=a$ 或 $a*c=a$。再根据吸收律，得到$(a*b)\oplus(a*c)=a$，从而 $a*(b\oplus c)=(a*b)\oplus(a*c)$。

同理可得到另一等式，所以线性序集 $\langle A, \leqslant\rangle$ 是分配格。**证毕。**

定理 8.8　$\langle A, \leqslant\rangle$ 是分配格。对于 A 中元素 a, b, c，如果 $a*c=b*c$，$a\oplus c=b\oplus c$，则 $a=b$。

证明　$\langle A, \leqslant\rangle$ 是分配格。利用$*$和$\oplus$运算的吸收律，分配律和交换律以及 $a*c=b*c$，$a\oplus c=b\oplus c$。有

$$\begin{aligned}a&=a*(a\oplus c)=a*(b\oplus c)\\&=(a*b)\oplus(a*c)=(a*b)\oplus(b*c)\\&=b*(a\oplus c)=b*(b\oplus c)=b.\end{aligned}$$

所以 $a=b$。**证毕。**

推论 8.1 在有界分配格 $\langle A, \leqslant\rangle$ 中，如果 A 的元素 a 有补元，那么它的补元是唯一的

证明 假设 a' 和 a'' 都是元素 a 的补元，即

$$a \oplus a' = 1,\ a * a' = 0.$$

$$a \oplus a'' = 1,\ a * a'' = 0.$$

那么 $a \oplus a' = a \oplus a''$, $a * a' = a * a''$。利用定理 8.8 知 $a' = a''$，即 a 的补元是唯一的。**证毕。**

定理 7.9 （摩根律）

$\langle A, \leqslant\rangle$ **是有界分配格，若 A 中元素 a, b 的补元分别为 a', b'，那么**

$$(a * b)' = a' \oplus b',$$

$$(a \oplus b)' = a' * b'.$$

证明

$$\begin{aligned}(a * b) \oplus (a' \oplus b') &= ((a * b) \oplus a') \oplus b' \\ &= (a' \oplus b) \oplus b' = 1,\end{aligned}$$

$$\begin{aligned}(a * b) * (a' \oplus b') &= a * (b * (a' \oplus b')) \\ &= a * (b * a') = 0.\end{aligned}$$

由推论 8.1 知 $(a * b)$ 的补元是唯一的，故 $(a * b)' = a' \oplus b'$。

同理可证 $(a \oplus b)' = a' * b'$。

定义 8.7 **有补分配格称为布尔格。**

8.2.4 模　　格

定义 8.8 **在格 $\langle A, \leqslant\rangle$ 中、对于 A 的任意元素 a, b, c，如果 $a \leqslant b$ 均使 $a \oplus (b * c) = b * (a \oplus c)$，那么称 $\langle A, \leqslant\rangle$ 为模格。**

特别地，如果 $\langle A, \leqslant\rangle$ 是分配格，若 $a \leqslant b$，则 $a \oplus b = b$，又

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c) = b * (a \oplus c),$$

所以每个分配格都是模格。

定理 8.10 **$\langle A, \leqslant\rangle$ 是模格的充要条件是对于 A 中任意元素 a, b, c，如果 $a \leqslant b$ 且 $a * c = b * c$，$a \oplus c = b \oplus c$，则必有 $a = b$。**

证明 已知 $\langle A, \leqslant\rangle$ 是模格，对于 A 中任意元素 a, b, c。若 $a\leqslant b$, $a*c=b*c$, $a\oplus c=b\oplus c$,那么必有

$$a=a\oplus(a*c)=a\oplus(b*c)=b*(a\oplus c)=b*(b\oplus c)=b.$$

反过来，由定理8.5知在格中 $a\leqslant b\Longleftrightarrow a\oplus(b*c)\leqslant b*(a\oplus c)$.我们令 $X=a\oplus(b*c)$, $Y=b*(a\oplus c)$,由 $a\leqslant b$ 知 $X\leqslant Y$。下面证明 $X\oplus c=Y\oplus c$, $X*c=Y*c$。

$$X\oplus c=(a\oplus(b*c))\oplus c=a\oplus((b*c)\oplus c)=a\oplus c.$$

$$Y\oplus c=(b*(a\oplus c))\oplus c.$$

由于 $a\leqslant b$, $a\leqslant a\oplus c$，有 $a\leqslant b*(a\oplus c)\leqslant a\oplus c$。根据定理8.3$\oplus$运算是保序的，由 $a\leqslant b*(a\oplus c)\leqslant a\oplus c$推出

$$a\oplus c\leqslant(b*(a\oplus c))\oplus c\leqslant a\oplus c\oplus c,$$

即

$$a\oplus c\leqslant Y\oplus c\leqslant a\oplus c.$$

由序关系 $\leqslant$ 的反对称性知 $Y\oplus c=a\oplus c$，从而 $X\oplus c=Y\oplus c$。

上面我们证明了在格中，当 $a\leqslant b$ 时。

$$(a\oplus(b*c))\oplus c=(b*(a\oplus c))\oplus c.$$

它的对偶命题是：当 $a\geqslant b$ 时，

$$(a*(b\oplus c))*c=(b\oplus(a*c))*c.$$

我们把后者的 a 与 b 交换位置，就得到，当 $b\geqslant a$ 时，

$$(b*(a\oplus c))*c=(a\oplus(b*c))*c.$$

这就是说，当 $a\leqslant b$ 时，$X*c=Y*c$。

现在有了 $X\leqslant Y$, $X\oplus c=Y\oplus c$, $X*c=Y*c$，从已知条件知必有 $X=Y$。也就是说，当 $a\leqslant b$ 时，$a\oplus(b*c)=b*(a\oplus c)$。所以格 $\langle A, \leqslant\rangle$ 是模格。

8.3 格——代数系统

我们知道集合以及集合上的一个或多个运算所组成的系统叫代数系统。前面几章介绍了群、环、域代数系统。格是不同于它们

的一个新的代数系统。

8.3.1 基本定义

定义 8.9 $*$ 和 $\oplus$ 是集合 A 上的两个二元运算。如果对于集合 A 的任意元素 a, b, c 满足

1° $(a*b)*c=a*(b*c)$， （结合律）

$(a\oplus b)\oplus c=a\oplus(b\oplus c)$。

2° $a*b=b*a$，$a\oplus b=b\oplus a$。 （交换律）

3° $a*(a\oplus b)=a$，$a\oplus(a*b)=a$， （吸收律）

那么称代数系统 $\langle A, *, \oplus\rangle$ 是格。

定理 8.11 定义 8.1 和定义 8.9 中定义的格是等价的。

证明 设 $\langle A, \leqslant\rangle$ 是定义 8.1 中定义的格，即对 A 中任意二元子集 $\{a, b\}$ 有唯一的最大下界和最小上界，分别记作 $a*b$ 和 $a\oplus b$。$*$ 和 $\oplus$ 是 A 上的两个二元运算。在定理 8.1 中已证明它们满足结合律、交换律和吸收律，所以 $\langle A, *, \oplus\rangle$ 也是定义 8.9 中定义的格。

若 $\langle A, *, \oplus\rangle$ 是定义 8.9 中定义的格，我们在 A 上定义关系 $\leqslant$。

$$a\leqslant b\Longleftrightarrow a*b=a。$$

当 $a*b=a$ 时，$a\oplus b=(a*b)\oplus b=b$，当 $a\oplus b=b$ 时，$a*b=a*(a\oplus b)=a$。故 $a*b=a\Longleftrightarrow a\oplus b=b$，即有

$$a\leqslant b\Longleftrightarrow a*b=a\Longleftrightarrow a\oplus b=b。$$

容易证明如此定义的关系 $\leqslant$ 是 A 上的部分序关系。

任取 A 中的元素 a, b，由于 $a*(a\oplus b)=a, b*(a\oplus b)=b$，知 $a\leqslant a\oplus b$，$b\leqslant a\oplus b$。于是 $a\oplus b$ 是 $\{a, b\}$ 的上界。如果 A 中元素 c 也是 $\{a, b\}$ 的上界，即 $a\leqslant c$，$b\leqslant c$，那么 $a\oplus c=c$，$b\oplus c=c$。

$$(a\oplus b)\oplus c=(a\oplus c)\oplus(b\oplus c)=c\oplus c=c，$$

这意味着 $a\oplus b\leqslant c$，从而 $a\oplus b$ 是 $\{a, b\}$ 的最小上界。

同理证明$a*b$是$\{a, b\}$的最大下界。$\langle A, \leqslant\rangle$是定义8.1中定义的格。

综上知这两个定义是等价的。

8.3.2 子格和格的直接积

定义 8.10 $\langle A, *, \oplus\rangle$是格，$B$是$A$的非空子集。如果集合$B$对$*$和$\oplus$运算是封闭的，那么称$\langle B, *, \oplus\rangle$是$\langle A, *, \oplus\rangle$的子格。

易看出，子格本身也是格。

例 1 Z^+是正整数集合，Z^+上定义二元运算

$$a*b=(a, b), \quad a\oplus b=[a, b]。$$

$\langle Z^+, *, \oplus\rangle$是格。令$T$令是偶正整数集合。由于两个偶数的最大公因子的仍是偶数，两个偶数的最小公倍数也是偶数，所以$\langle T, *, \oplus\rangle$是$\langle Z^+, *, \oplus\rangle$的子格。

例 2 $\langle A, *, \oplus\rangle$是格，$A$中的元素$a, b, a\leqslant b$，令

$$I[b, a]=\{x \mid x\in A, a\leqslant x\leqslant b\}。$$

任取$x_1, x_2\in I[b, a]$，$a\leqslant x_1, x_2\leqslant b$，即

$$\begin{aligned} &a*x_i=a, \quad x_i*b=x_i, \\ &a\oplus x_i=x_i, \quad x_i\oplus b=b, \end{aligned} \qquad 1\leqslant i\leqslant 2。$$

那么

$$\begin{aligned} &a*(x_1*x_2)=(a*x_1)*x_2=a*x_2=a, \\ &(x_1*x_2)*b=x_1*(x_2*b)=x_1*x_2, \end{aligned}$$

即$a\leqslant x_1*x_2\leqslant b$，$x_1*x_2\in I[b, a]$。

同理可证$a\leqslant x_1\oplus x_2\leqslant b$，$x_1\oplus x_2\in I[b, a]$。从而$\langle I[b, a], *, \oplus\rangle$是$\langle A, *, \oplus\rangle$的子格。

例 3 $\langle \mathscr{P}(\{1, 2, 3\}), \cap, \cup\rangle$是格。令

$$A_1=\{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\},$$

$$A_2=\{\phi, \{1\}, \{3\}, \{1, 3\}\},$$

$$A_3=\{\phi, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\},$$

$\langle A_1, \cap, \cup\rangle$ 和 $\langle A_2, \cap, \cup\rangle$ 是 $\langle \mathscr{P}(\{1, 2, 3\}), \cap, \cup\rangle$ 的子格。而 A_3 中 $\{1, 2\}\cap\{2, 3\}=\{2\}\notin A_3$，$A_3$ 不是 $\mathscr{P}(A)$ 的子格。由此看出并非 A 的每个子集都构成格 $\langle A, *, \oplus\rangle$ 的子格。

定义 8.11 $\langle A, *, \oplus\rangle$ 和 $\langle A_2, \wedge, \vee\rangle$ **是两个格，构造一个新的代数系统** $\langle A_1\times A_2, \cdot, +\rangle$，**其中·和+运算的定义是：** $(a_1, a_2), (b_1, b_2)\in A_1\times A_2$，

$$(a_1, a_2)\cdot(b_1, b_2)=(a_1 * b_1, a_2\wedge b_2),$$

$$(a_1, a_2)+(b_1, b_2)=(a_1\oplus b_1, a_2\vee b_2).$$

我们称 $\langle A_1\times A_2, \cdot, +\rangle$ 是 $\langle A_1, *, \oplus\rangle$ 和 $\langle A_2, \wedge, \vee\rangle$ 的直接积。

在此定义中，$A_1\times A_2$ 中元素的 · 和 + 运算是由第一分量按 A_1 中的 $*$ 和 $\oplus$ 运算，第二分量按 A_2 中的 $\wedge$ 和 $\vee$ 运算来实现的。$\langle A_1, *, \oplus\rangle$ 和 $\langle A_2, \wedge, \vee\rangle$ 是格，所以 $A_1\times A_2$ 中的 · 和 + 运算也满足结合律，交换律和吸收律。从而两个格的直接积也是格，并且是用规模小的格构造成规模大的格。

例 1 $A=\{0, 1\}$，在 A 上定义关系 $\leqslant_1$，$a, b\in A$，

$$a\leqslant_1 b\Longleftrightarrow a\leqslant b.$$

$\langle A, \leqslant_1\rangle$ 是格。在 A^2 上定义关系 $\leqslant_2$，$(a, b), (c, d)\in A^2$，

$$(a, b)\leqslant_2(c, d)\Longleftrightarrow a\leqslant_1 c,\ b\leqslant_1 d,$$

$\langle A^2, \leqslant_2\rangle$ 是 $\langle A, \leqslant_1\rangle$ 与 $\langle A, \leqslant_1\rangle$ 两个格的直接积。类似地在 A^3 上定义关系 $\leqslant_3$，$(a, b, c), (d, e, f)\in A^3$，

$$(a, b, c)\leqslant_3(d, e, f)\Longleftrightarrow a\leqslant_1 d,\ b\leqslant_1 e,\ c\leqslant_1 f,$$

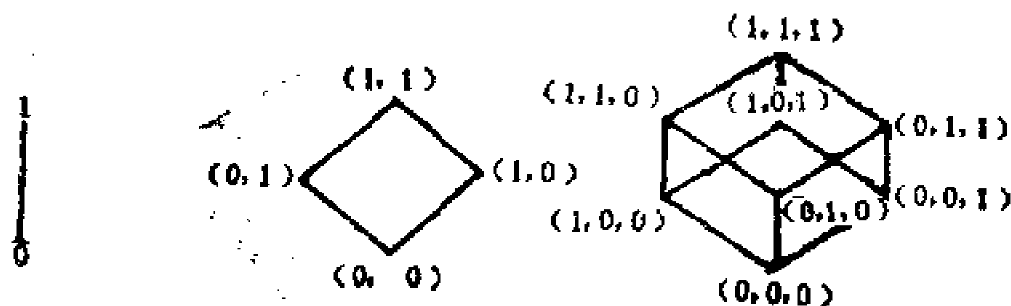


图 20

$\langle A^3, \leqslant_3\rangle$ 是 $\langle A, \leqslant_1\rangle$ 与 $\langle A^2, \leqslant_2\rangle$ 两个格的直接积. 它们的 Hasse 图是图 20。

8.3.3 格的同态与同构

定义 8.12 $\langle A_1, *, \oplus\rangle$ 和 $\langle A_2, \wedge, \vee\rangle$ 是两个格，如果存在从 A_1 到 A_2 的映射 f: $A_1 \to A_2$，对于 A_1 中任意元素 a, b，

$$f(a*b)=f(a)\wedge f(b),$$
$$f(a\oplus b)=f(a)\vee f(b),$$

则称 f 是从 A_1 到 A_2 的格同态映射。

若 f 是从 A_1 到 A_2 的格同态映射，并且为双射，则称 f 是从 A_1 到 A_2 的格同构映射。如果两个格之间存在着格同构映射，那么称这两个格是同构的。

在格 $\langle A_1, *, \oplus\rangle$ 中，$a\leqslant_1 b \Longleftrightarrow a*b=a$。$f$ 是从 $\langle A_1, *, \oplus\rangle$ 到 $\langle A_2, \wedge, \vee\rangle$ 的格同态映射，

$$f(a)=f(a*b)=f(a)\wedge f(b),$$

所以 $f(a)\leqslant_2 f(b)$，即格的同态映射是一种保序映射。反过来不一定成立。例如 $A_1=A_2=\{1, 2, 3, 4, 6, 12\}$。$\langle A_1, \leqslant_1\rangle$ 和 $\langle A_2, \leqslant_2\rangle$ 是格，它们的 Hasse 图是图 21。

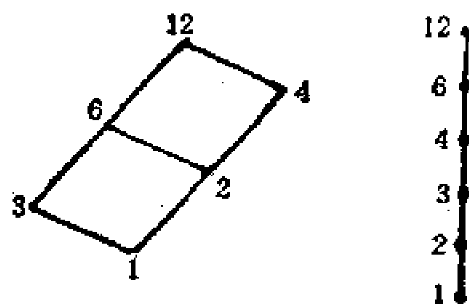


图 21

令 $f: A_1\to A_2, f(x)=x$ 是保序映射，但是它不是同态映射，因为

$$f(3*4)=f(1)=1,$$
$$f(3)\wedge f(4)=3\wedge 4=3。$$

定理 8.12 f 是从集合 A_1 到集合 A_2 的双射。f 是从格 $\langle A_1, \leqslant_1\rangle$ 到格 $\langle A_2, \leqslant_2\rangle$ 的同构映射当且仅当对于 A_1 的元素 a, b，

$$a\leqslant_1 b \Longleftrightarrow f(a)\leqslant_2 f(b)。$$

证明 已知 f 是从 A_1 到 A_2 的格同构映射。在格 $\langle A_1, \leqslant_1\rangle$ 中 $a\leqslant_1 b\Longleftrightarrow a*b=a$。当 $a*b=a$ 时，

$$f(a*b)=f(a)\cdot f(b)=f(a),$$

故 $f(a)\leqslant_2 f(b)$。又当 $f(a)\leqslant_2 f(b)$ 时，
因 f 是单射，故 $a=a*b$。从而 $a*b=a\Longleftrightarrow f(a)\leqslant_2 f(b)$。最后得

$$f(a)=f(a)\cdot f(b)=f(a*b).$$

到 $a\leqslant_1 b\Longleftrightarrow f(a)\leqslant_2 f(b)$。

反过来，已知 $f: A_1\to A_2$ 是双射。任取 $a, b\in A_1$，$a*b\leqslant_1 a$，$a*b\leqslant_1 b$，由于 f 保序，得到 $f(a*b)\leqslant_2 f(a)$，$f(a*b)\leqslant_2 f(b)$。从而 $f(a*b)\leqslant_2 f(a)\cdot f(b)$。任取 $x,y\in A_2$，由于 f 是满射，存在 $a, b\in A_1$ 使 $f(a)=x$，$f(b)=y$。A_2 是格，$x\cdot y=f(a)\cdot f(b)\in A_2$，那么存在 $c\in A_1$ 使 $f(c)=x\cdot y=f(a)\cdot f(b)$。于是有 $f(c)\leqslant_2 f(a)$，$f(c)\leqslant_2 f(b)$，由于 f 是保序的，$c\leqslant_1 a$，$c\leqslant_1 b$，从而 $c\leqslant_1 a*b$。再用 f 的保序性得到 $f(a)\cdot f(b)=f(c)\leqslant f(a*b)$。综上最后得到 $f(a)\cdot f(b)=f(a*b)$。同理可证 $f(a)+f(b)=f(a\oplus b)$。所以 f 是格同构映射。

引理 8.1 格 $\langle A, *, \oplus\rangle$ 是模格当且仅当 A 的每个 $I[b, a]=\{x|x\in A, a\leqslant x\leqslant b\}$ 中如果有两个元素可比较且有公共补元，那么这两个元素必相等。

证明 如果在格 $\langle A, *, \oplus\rangle$ 中，$u\leqslant v$，$I[u, v]$ 中有两个可比较但不相等的元素 $a_0<b_0$，它们有一个公共补元 c，即

$$a_0*c=b_0*c=u,\quad a_0\oplus c=b_0\oplus c=v,\qquad u\leqslant a_0<b_0\leqslant v.$$

那么

$$a_0\oplus(b_0*c)=a_0\oplus u=a_0<b_0=b_0*v=b_0*(a_0\oplus c),$$

也就是说 $a_0<b_0$。但是 $a_0\oplus(b*c)\neq b*(a\oplus c)$，所以 $\langle A, *, \oplus\rangle$ 不是模格。这意味着，如果格 $\langle A, *, \oplus\rangle$ 是模格，则 A 的每个 $I[b, a]$ 里，若有两个可比较元素有公共补元，则这两个元素必相等。

如果格 $\langle A, *, \oplus\rangle$ 不是模格，那么必存在 $a_0, b_0\in A$，且

$a_0 < b_0$，使得 $a_0 \oplus (b_0 * c) < b_0 * (a_0 \oplus c)$。令 $x = a_0 \oplus (b_0 * c)$，$y = b_0 * (a_0 \oplus c)$，显然 $a_0 \leqslant x$，$y \leqslant b_0$，$b_0 * c \leqslant x < y \leqslant a_0 \oplus c$，$b_0 * c \leqslant c \leqslant a_0 \oplus c$，

$$c * y = c * b_0 * (a_0 \oplus c) = c * b_0.$$

由于 $y \leqslant a_0 \oplus c$，$a_0 < y$，

$$c \oplus y \leqslant c \oplus (a_0 \oplus c) = a_0 \oplus c \leqslant y \oplus c,$$

得到

$$c \oplus y = a_0 \oplus c.$$

同理可证 $x * c = b_0 * c$，$x \oplus c = a_0 \oplus c$。这说明在 $I[a_0 \oplus c, b_0 * c]$ 中 $x < y$，x 与 y 有公共补元 c。证毕。

用这个引理可以证明

定理 8.13　格是模格当且仅当它不包含一个 5 元子格与图 22 同构。

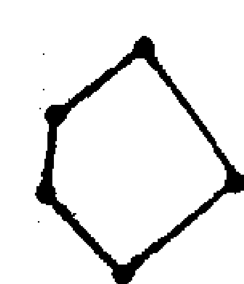


图 22

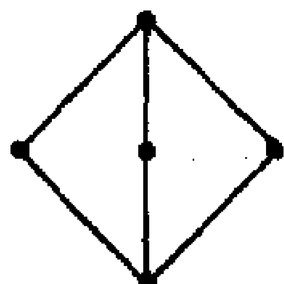


图 23

与此类似的定理我们不加以证明只叙述如下。

定理 8.14　格是分配格当且仅当该格是模格且不包含一个 5 元子格与图 23 同构。

8.4 布 尔 代 数

8.4.1 布 尔 代 数

在格中可以定义 $*$ 和 $\oplus$ 两个二元运算。在有补分配格中，每个元素有补元且补元唯一，这样就可以在有补分配格中定义求补运算。另外它有最大元 1 和最小元 0。所以布尔格可以看成代数系统 $\langle A, *, \oplus, ', 1, 0\rangle$，并称为由布尔格 $\langle A, \leqslant\rangle$ 诱导出来的代数系统。

定义 8.13　设 A 是至少有两个元素的集合，$*$ 和 $\oplus$ 是 A 上

的二元运算．对于 A 的任意元素 a, b, c，如果

1° $a*b=b*a$,

$a\oplus b=b\oplus a$,

2° $a*(b\oplus c)=(a*b)\oplus(a*c)$,

$a\oplus(b*c)=(a\oplus b)*(a\oplus c)$,

3° $0,1\in A$，对 A 中任意元素 a，$a*1=a$，$a\oplus 0=a$，

4° 对 A 中任意元素 a，存在 $a'\in A$，使 $a*a'=0$，$a\oplus a'=1$，

则称 $\langle A, *, \oplus, ', 0, 1\rangle$ 为布尔代数。

显然由布尔格诱导出来的代数系统为布尔代数。

定理 8.15 布尔代数 $\langle A, *, \oplus, ', 1, 0\rangle$ **相应的** $\langle A, *, \oplus\rangle$ **是布尔格。**

证明 由布尔代数定义看出，我们要证明 $\langle A, *, \oplus\rangle$ 是布尔格，只需证明 $\langle A, *, \oplus\rangle$ 是格，并且 0 和 1 分别是该格的最小元和最大元。

已知 $\langle A, *, \oplus, ', 0, 1\rangle$ 是布尔代数，在代数系统 $\langle A, *, \oplus\rangle$ 中，二元运算 $*, \oplus$ 满足交换律，任取 $a, b\in A$，

$$
\begin{aligned}
a*(a\oplus b) &= (a\oplus 0)*(a\oplus b)=a\oplus(0*b)\\
&= a\oplus((0*b)\oplus(b'*b))=a\oplus((0\oplus b')*b)\\
&= a\oplus(b'*b)=a\oplus 0=a.
\end{aligned}
$$

同理可证 $a\oplus(a*b)=a$。所以二元运算 $*, \oplus$ 满足吸收律。又令 $x=a*(b*c)$，$y=(a*b)*c$，显然

$$
x=x\oplus 0=x\oplus(a*a')=(x\oplus a)*(x\oplus a'),
$$

$$
y=y\oplus 0=y\oplus(a*a')=(y\oplus a)*(y\oplus a'),
$$

其中

$$
x\oplus a=(a*(b*c))\oplus a=a,
$$

$$
y\oplus a=((a*b)*c)\oplus a=((a*b)\oplus a)*(a\oplus c)=a*(a\oplus c)=a,
$$

$$
x\oplus a'=(a*(b*c))\oplus a'=(b*c)\oplus a',
$$

$$
y\oplus a'=((a*b)*c)\oplus a'=((a*b)\oplus a')*(c\oplus a')
$$

$$= (b \oplus a') * (c \oplus a') = (b * c) \oplus a',$$

于是由 $x \oplus a = y \oplus a$，$x \oplus a' = y \oplus a'$ 推出 $x = y$，即

$$a * (b * c) = (a * b) * c.$$

同理可证 $a \oplus (b \oplus c) = (a \oplus b) \oplus c$。所以二元运算 $*$，$\oplus$ 满足结合律。从而 $\langle A, *, \oplus \rangle$ 是格。在布尔代数 $\langle A, *, \oplus, ', 0, 1 \rangle$ 中，对任意元素 $a \in A$ 均有

$$a * 1 = a, \quad a \oplus 0 = a.$$

在 $\langle A, *, \oplus \rangle$ 中的序关系是，$a, b \in A$，

$$a \leqslant b \Longleftrightarrow a \oplus b = b \Longleftrightarrow a * b = a.$$

于是在格 $\langle A, *, \oplus \rangle$ 中 $0 \leqslant a$，$a \leqslant 1$，即 0 和 1 分别是该格的最小元和最大元。

综上分析知 $\langle A, *, \oplus \rangle$ 是布尔格。**证毕。**

从这个定理可以看出在有补分配格中，存在最小元和最大元每个元素有补，运算满足交换律和结合律是其最核心的性质。

8.4.2 布尔代数的子代数

定义 8.14 设 A_1 是布尔代数 $\langle A, *, \oplus, ', 0, 1 \rangle$ 中集合 A 的子集。如果 $0, 1 \in A_1$ 并且 A_1 对于 $*$，$\oplus$，$'$ 运算是封闭的，那么称 A_1 是 A 的子代数。

例 1 $A = \{1, 2, 3\}$，$\langle \mathscr{P}(A), \subseteq \rangle$ 是有补分配格，其上的 $*$，$\oplus$，$'$ 运算分别为 $\cap$，$\cup$，$-$ 运算。最小元和最大元分别为 ϕ，A，故 $\langle \mathscr{P}(A), \cap, \cup, -, \phi, A \rangle$ 是布尔代数。令 $A_1 = \{\phi, \{1\}, \{2, 3\}, A\}$，则 A_1 是 A 的子代数。

例 2 $\langle A, *, \oplus, ', 0, 1 \rangle$ 是布尔代数。a, b 是 A 中元素且 $a \leqslant b$，定义 A 的子集合。

$$I[b, a] = \{x \mid x \in A, a \leqslant x \leqslant b\}.$$

前面已经证明 $I[b, a]$ 对运算 $*$，$\oplus$ 是封闭的。由于 $\langle A, *, \oplus \rangle$ 是分配格，所以 $\langle I[b, a], *, \oplus \rangle$ 也是分配格。但是 $I[b, a]$，的最大元是 a，最小元是 b，与布尔代数的最大元和最小元不同，

另外 $I[b, a]$对求补运算不一定封闭，故 $I[b, a]$不是 A 的子代数。

在 $I[b, a]$中的 x，定义 $\bar{x}=(a\oplus x')*b$。显然有$\bar{x}\leqslant b$，

$$\bar{x}*a=(a\oplus x')*b*a=a*b=a,$$

故 $a\leqslant\bar{x}$，而

$$\bar{x}\oplus x=((a\oplus x')*b)\oplus x=x\oplus b=b,$$

$$\bar{x}*x=((a\oplus x')*b)*x=a*x*b=a,$$

说明 $\bar{x}$ 是 x 的补元。从而$\langle I[b, a], *, \oplus, -, a, b\rangle$ 是布尔代数，但不是 $\langle A, *, \oplus, ', 0, 1\rangle$ 的子代数。

8.4.3 布尔代数的同态与同构

定义 8.15 $\langle A_1, *, \oplus, ', 0, 1\rangle$ 与 $\langle A_2, \wedge, \vee, ^-, \tilde{0}, \tilde{1}\rangle$ **是布尔代数。对于映射** $f: A_1\to A_2$，**如果** a, b **是** A_1 **中任意元素，**

$$f(a*b)=f(a)\wedge f(b),$$

$$f(a\oplus b)=f(a)\vee f(b),$$

$$f(a')=\overline{f(a)},$$

那么称 f **是同态映射。**

特别当 f 是双射时，称 f 为同构映射。并说布尔代数 A_1 与 A_2 同构。

定理 8.16 $\langle A, *, \oplus, ', 0, 1\rangle$ **是布尔代数，对于** A **的任意元素** a，**布尔代数** $I[a', 0]$**与布尔代数** $I[1, a]$**是同构的。**

证明 任取 $a\in A$，$a'\in A$ 且 $0\leqslant a'\leqslant 1$。

$$I[a', 0]=\{x\mid x\in A, 0\leqslant x\leqslant a'\},$$

$$I[1, a]=\{x\mid x\in A, a\leqslant x\leqslant 1\}.$$

当 $x\in I[a', 0]$ 时，$0\leqslant x\leqslant a'$，由于$\oplus$运算是保序的，即 $0\oplus a\leqslant x\oplus a\leqslant a'\oplus a$，故 $a\leqslant x\oplus a\leqslant 1$，即 $x\oplus a\in I[1, a]$。现令 $f: I[a', 0]\to I[1, a]$，$f(x)=x\oplus a$。任取 $y\in I[1, a]$，令 $x=y*a'$，因 $a\leqslant y\leqslant 1$ 并且 $*$ 是保序的，故 $0=a*a'\leqslant x=y*a'\leqslant 1*a'=a'$，即 $0\leqslant$

$x \leqslant a'$。$f(x)=x\oplus a=(y*a')\oplus a=y\oplus a=y$，这表明 x 是 y 的原象，所以 f 是满射。又若 $x_1,x_2\in I[a',0]$是 $y\in I[1,a]$的原象，即 $f(x_1)=x_1\oplus a=x_2\oplus a=f(x_2)$。

$$x_1=x_1*a'=(x_1\oplus a)*a'=(x_2\oplus a)*a'=x_2*a'=x_2,$$

这表明 f 是单射。从而 f 是从 $I[a',0]$到 $I[1,a]$的双射。

任取 $x_1,x_2\in I[a',0]$，

$$f(x_1*x_2)=(x_1*x_2)\oplus a=(x_1\oplus a)*(x_2\oplus a)=f(x_1)*f(x_2),$$

$$f(x_1\oplus x_2)=(x_1\oplus x_2)\oplus a=(x_1\oplus a)\oplus(x_2\oplus a)$$
$$=f(x_1)\oplus f(x_2),$$

$$f(\overline{x}_1)=f((0\oplus x_1')*a')=(x_1'*a')\oplus a=x_1'\oplus a,$$

$$\overline{f(x_1)}=\overline{x_1\oplus a}=(a\oplus(x_1\oplus a)')*1=a\oplus(x_1'*a')=x_1'\oplus a.$$

综上分析 f 是同构映射，$I[a',0]\cong I[1,a]$。

定义 8.16 $\langle A_1,*,\oplus,',0,1\rangle$ **和** $\langle A_2,\wedge,\vee,^-,\tilde{0},\tilde{1}\rangle$ **是布尔代数。在** $A_1\times A_2$ **上定义** $\tilde{*}$，$\tilde{\oplus}$，^{0}，**运算**，(a_1,a_2)，$(b_1,b_2)\in A_1\times A_2$，

$$(a_1,a_2)^0=(a_1',\bar{a}_2),$$

$$(a_1,a_2)\tilde{*}(b_1,b_2)=(a_1*b_1,a_2\wedge b_2),$$

$$(a_1,a_2)\tilde{\oplus}(b_1,b_2)=(a_1\oplus b_1,a_2\vee b_2),$$

称 $\langle A_1\times A_2,\tilde{*},\tilde{\oplus},^0,(0,\tilde{0}),(1,\tilde{1})\rangle$ **是布尔代数** A_1 **与** A_2 **的直积。**

容易证明两个布尔代数的直积仍是布尔代数。证明留作习题。

定理 8.17 $\langle A,*,\oplus,',0,1\rangle$ **是布尔代数，**a **是** A **中的元素，**A **与直积** $\tilde{A}=I[a,0]\times I[1,a]$**同构。**

证明 任取 $x\in A$，即 $0\leqslant x\leqslant 1$，由于 $*$，$\oplus$ 运算是保序的，故 $0=0*a\leqslant x*a\leqslant 1*a=a$，$a=0\oplus a\leqslant x\oplus a\leqslant 1\oplus a=1$。现定义 f：$A\to I[a,0]\times I[1,a]$，$f(x)=(x*a,x\oplus a)$。任取 $x_1,x_2\in A$，

$$f(x_1\oplus x_2)=((x_1\oplus x_2)*a,(x_1\oplus x_2)\oplus a)$$
$$=((x_1*a)\oplus(x_2*a),(x_1\oplus a)\oplus(x_2\oplus a))$$

$$= (x_1 * a, x_1 \oplus a) \oplus (x_2 * a, x_2 \oplus a) = f(x_1) \oplus f(x_2).$$

$$f(x_1 * x_2) = ((x_1 * x_2) * a, (x_1 * x_2) \oplus a)$$
$$= ((x_1 * a) * (x_2 * a), (x_1 \oplus a) * (x_2 \oplus a))$$
$$= (x_1 * a, x_1 \oplus a) * (x_2 * a, x_2 \oplus a) = f(x_1) * f(x_2).$$

$$\overline{f(\bar{x})} = (\overline{x * a}, \overline{x \oplus a}) = (0 \oplus (x * a)') * a, (a \oplus (x \oplus a)' * 1)$$
$$= ((x' \oplus a') * a, a \oplus (x' * a'))$$
$$= (x' * a, x' \oplus a) = f(x'),$$

所以 f 是同态映射。

任取 $(y, z) \in I[a, 0] \times I[1, a]$，$0 \leqslant y \leqslant a$，$a \leqslant z \leqslant 1$，令 $x = y \oplus (z * a') \in A$，

$$f(x) = f(y \oplus (z * a'))$$
$$= ((y \oplus (z * a')) * a, (y \oplus (z * a')) \oplus a)$$
$$= (y * a, y \oplus z \oplus a) = (y, z).$$

x 是 (y, z) 的原象，故 f 是满射。又设 $x_1, x_2 \in A$ 都是 $(y, z) \in I[a, 0] \times I[1, a]$ 的原象，即

$$f(x_1) = (x_1 * a, x_1 \oplus a) = (x_2 * a, x_2 \oplus a) = f(x_2),$$

那么

$$x_1 = x_1 * (a \oplus a') = (x_1 * a) \oplus (x_1 * a')$$
$$= (x_1 * a) \oplus ((x_1 \oplus a) * a') = (x_2 * a) \oplus ((x_2 \oplus a) * a')$$
$$= x_2 * (a \oplus a') = x_2,$$

故 f 是单射。从而 f 是双射，A 与 $\tilde{A}$ 是同构的。**证毕**

例 1 设 $A = \{1, 2, \cdots, n\}$，$A_1 = \{1, 2, \cdots, k\}$，$\bar{A}_1 = \{k+1, k+2, \cdots, n\}$。$\langle \mathscr{P}(A), \cap, \cup, ^-, \phi, A \rangle$ 是布尔代数。

$$I[A_1, \phi] = \{x \mid x \in \mathscr{P}(A), \phi \subseteq x \subseteq A_1\} = \mathscr{P}(A_1).$$
$$I[A, A_1] = \{x \mid x \in \mathscr{P}(A), A_1 \subseteq x \subseteq A\} = \mathscr{P}(\bar{A}_1)$$

由定理 8.16 知 $I[\bar{A}_1, \phi] \cong I[A, A_1]$。又由定理 8.17 知 $\mathscr{P}(A) \cong I[A_1, \phi] \times I[\bar{A}_1, \phi] = \mathscr{P}(A_1) \times \mathscr{P}(\bar{A}_1)$。

定理 8.18 A **是有限布尔代数，**$|A| = 2^n$。**令** $B = \{1, 2, \cdots, n\}$，**则** A **与** $\langle \mathscr{P}(B), \cap, \cup, ^-, \phi, B \rangle$ **两个布尔代数同构。**

证明 我们对集合 A 的元素个数进行归纳证明。当 $|A|=2$ 时，$A=\{0,1\}$，$f: A\to\mathscr{P}(\{1\})$，$f(0)=\phi$，$f(1)=\{1\}$。$f$ 是同构映射 $A\cong\mathscr{P}(\{1\})$。假设 $|A|<k$ 时命题成立。现 $|A|=k$，取 $a\in A$ 且 $0<a<1$，从定理 8.18 知 $A\cong I[a,0]\times I[1,a]$。又从定理 8.16 知 $A\cong I[a,0]\times I[a',0]$。由于 $|I[a,0]|<k$，$|I[a',0]|<k$。由归纳假设得知布尔代数 $I[a,0]$ 和 $I[a',0]$ 分别与 $\mathscr{P}(B_1)$ 和 $\mathscr{P}(B_2)$ 同构，其中 $|B_1|=k_1$，$|B_2|=k_2$，

$$|A|=|I[a,0]\times I[a',0]|=2^{k_1}\cdot 2^{k_2}=2^{k_1+k_2}.$$

从上面例 1 知若 $A\cong\mathscr{P}(B_1)\times\mathscr{P}(B_2)$，那么存在 k_1+k_2 个元素的集合 B 使得 $A\cong\mathscr{P}(B)$。**证毕。**

由这个定理看出，$|A|=n$，$\langle\mathscr{P}(A),\cap,\cup,{}^-,\phi,A\rangle$ 是有 2^n 个元素的布尔代数。它穷尽了所有有限布尔代数。

8.4.4 布尔代数的原子表示

如果在格 $\langle A,\leqslant\rangle$ 中有最小元 0，那么该最小元的控制元素称为原子。

在格 $\langle A,\leqslant\rangle$ 的 Hasse 图（图 24）中 $a_1, a_2, \cdots, a_k$ 是它的原子。显然 $a_i * a_j=0\ (i\neq j)$。

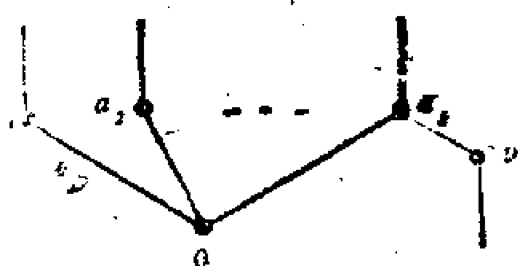


图 24

引理 8.1 $\langle A,\leqslant\rangle$ **是有限格，0 是它的最小元。对于 A 中任意非零元素 b，至少存在一个原子 a 使得 $a\leqslant b$。**

证明 对于有限格 $\langle A,\leqslant\rangle$ 中任意非零元素 b 有以下两种情况：

1° b 本身是原子，那么显然 $b\leqslant b$。

2° b 不是原子，0 是有限格 $\langle A,\leqslant\rangle$ 的最小元，即 $0<b$。b 不是 0 的控制元素，那么必然存在 $b_1\in A$ 使得 $0<b_1<b$。对于 b_1 又有两种情况：

1）b_1 是原子，取 $a=b_1$ 即可。

2) b_1 不是原子，0 是 $\langle A, \leqslant\rangle$ 的最小元，即 $0<b_1$。b_1 不是 0 的控制元素，那么必然存在 $b_2 \in A$ 使得 $0<b_2<b_1<b$。这里 $b_2 \neq b$。…

由于 A 是有限集合，这个过程不可能无限地进行下去。也就是说，在有限步之后 b_t 本身就是原子，取 $a=b_t$ 即可。**证毕。**

引理 8.2 $\langle A, *, \oplus, ', 0, 1\rangle$ **是有限布尔代数。b 是 A 中的非零元素，若 $a_1, a_2, \cdots, a_k$ 是 A 中满足 $a_i \leqslant b$ 的所有原子，则 $b=a_1 \oplus a_2 \oplus \cdots \oplus a_k$。**

证明 $a_1, a_2, \cdots, a_k$ 是 A 的原子并且 $a_i \leqslant b$, $1 \leqslant i \leqslant k$。显然 $a_1 \oplus a_2 \oplus \cdots \oplus a_k \leqslant b$。下面我们要证明 $b \leqslant a_1 \oplus a_2 \oplus \cdots \oplus a_k$。由于在有补分配格中 $c \leqslant d \Longleftrightarrow c * d'=0$（作为习题已证明），所以只需证明 $b *\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right)'=0$。我们用反证法。如若不然，$b *\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right)' \neq 0$，由引理 8.1 知存在原子 a 使得 $a \leqslant b *\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right)'$。这里 a 是原子且 $a \leqslant b$, $a \leqslant\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right)'$，而 $a_1, a_2, \cdots, a_k$ 是小于 b 的全部原子，故 $a \in\left\{a_1, a_2, \cdots, a_k\right\}$。从而 $a \leqslant a_1 \oplus a_2 \oplus \cdots \oplus a_k$。从而 $a \leqslant\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right) *\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right)'=0$。这与 a 是原子矛盾，故不可。所以必有 $b *\left(a_1 \oplus a_2 \oplus \cdots \oplus a_k\right)'=0$。

以上证明表明 A 的非零元素可以表示成满足 $a_i \leqslant b$ 的所有原子 $a_1, a_2, \cdots, a_k$ 之和。下面将证明这种表示形式是唯一的。假设 $b_1, b_2, \cdots, b_l$ 是原子并且。$b=b_1 \oplus b_2 \oplus \cdots \oplus b_l$。由运算 $\oplus$ 的定义知 $b_1, b_2, \cdots, b_l \leqslant b$ 且 $b_1, b_2, \cdots, b_l$ 是原子，而 $\left\{a_1, a_2, \cdots, a_k\right\}$ 是小于 b 的全部原子，故 $\left\{b_1, b_2, \cdots, b_l\right\} \subseteq\left\{a_1, a_2, \cdots, a_k\right\}$。如果 $l<k$，即存在 $a_m \notin\left\{b_1, b_2, \cdots, b_l\right\}$，

$$
\begin{aligned}
a_m=a_m * b & =a_m *\left(b_1 \oplus b_2 \oplus \cdots \oplus b_l\right) \\
& =\left(a_m * b_1\right) \oplus\left(a_m * b_2\right) \oplus \cdots \oplus\left(a_m * b_l\right),
\end{aligned}
$$

其中 $a_m \neq b_i$，a_m 与 b_i 都是原子，$a_m * b_i=0$，$1 \leqslant i \leqslant l$。从而推出 $a_m=0$。这与 a_m 是原子矛盾，故不可，所以 $l=k$，即 b 表示成原子之和的形式是唯一的。**证毕。**

引理 8.3　在布尔格 $\langle A, \leqslant\rangle$ 中若任取非零元素 b 和原子 a，则或者 $a\leqslant b$，或者 $a\leqslant b'$，两者必居取一。

证明　b 和 a 分别是 A 的非零元素和原子。显然 $0\leqslant a*b\leqslant a$。由于 a 是原子，即 a 是 0 的控制元素，不可能有非零元素 $a*b$ 使得 $0<a*b<a$。如果 $a*b=a$，则 $a\leqslant b$。又在布尔格中 $a\leqslant b'$ 当且仅当 $a*(b')'=0$，即 $a*b=0$。所以当 $a*b=0$ 时，必有 $a\leqslant b'$。而 $a\leqslant b, a\leqslant b'$ 与不可能同时成立，否则 $a\leqslant b*b'=0$ 与 a 是原子矛盾。所以 $a\leqslant b$ 与 $a\leqslant b'$ 两者必居其一。**证毕。**

定理 8.19　$\langle A, *, \oplus, ', 0, 1\rangle$ **是有限布尔代数，若** S **是** A **中所有原子所构成的集合，那么** $\langle A, *, \oplus, ', 0, 1\rangle$ **与** $\langle \mathscr{P}(S), \cap, \cup, ^{-}, \phi, S\rangle$ **同构。**

证明　在两个布尔代数之间构作映射 $f: A\to\mathscr{P}(S)$，对任意 $a\in A$，

$$f(a)=\begin{cases}\phi, & a=0,\\ \{a_1, a_2, \cdots, a_k \mid a_i\in S, a_i\leqslant a, 1\leqslant i\leqslant k\}, & a\neq 0.\end{cases}$$

由引理 8.2 知对于A中有非零元素 a 它的像 $f(a)$是唯一确定的。任取$\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}\subseteq S$，$\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}\neq\phi$，令 $b=a_{i_1}\oplus a_{i_2}\oplus\cdots\oplus a_{i_p}\in A$，$f(b)=\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}$，故 b 是 $\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}$的原象。$f$ 是满射。假设 a，b 都是 $\{a_{i_1}, a_{i_2}, \cdots, a_{i_p}\}$的原象，由引理 8.2 知 $a=a_{i_1}\oplus a_{i_2}\oplus\cdots\oplus a_{i_p}=b$，所以 f 是单射。综上知 f 是双射。

下面证明 f 保持 $*$，$\oplus$，$'$ 运算。

1°　当 $a=0$ 或 $b=0$ 时，$a*b=0$，$f(a*b)=\phi$，$f(a)=\phi$ 或 $f(b)=\phi$，所以 $f(a)\cap f(b)=\phi$。从而 $f(a*b)=f(a)\cap f(b)$。

当 $a\neq 0$ 且 $b\neq 0$ 时，$f(a)=\{a_1, a_2, \cdots, a_k\}$，$f(b)=\{b_1, b_2, \cdots, b_l\}$。也就是说 $a_1, a_2, \cdots, a_k$ 是小于 a 的全部原子，$b_1, b_2, \cdots, b_l$ 是小于 b 的全部原子。如果 $a*b=0$，显然 $f(a*b)=\phi$。假若 $f(a)\cap f(b)\neq\phi$，即存在 $x\in f(a)\cap f(b)$，x 是小于 a 的原子也是小于 b 的原子，那么 $x\leqslant a*b=0$。这与 x 是原子矛盾，

故不可。所以 $f(a*b)=f(a)\cap f(b)=\phi$。如果 $a*b\neq 0$，令 $f(a*b)=\{c_1,c_2,\cdots,c_m\}$，$c_1,c_2,\cdots,c_m$ 是小于 $a*b$ 的全部原子。由于 $c_i\leqslant a*b\leqslant a$，$c_i\leqslant a*b\leqslant b$，必有 $c_i\in\{a_1,a_2,\cdots,a_k\}$，$c_i\in\{b_1,b_2,\cdots,b_l\}$，$1\leqslant i\leqslant m$。从而

$$\{c_1,c_2,\cdots,c_m\}\subseteq\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}.$$

反过来，任取 $x\in\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}$，$x\leqslant a$ 且 $x\leqslant b$，于是 $x\leqslant a*b$。所以 $x\in\{c_1,c_2,\cdots,c_m\}$。它表明

$$\{a_1,a_2,\cdots a_k\}\cap\{b_1,b_2,\cdots,b_l\}\subseteq\{c_1,c_2,\cdots,c_m\}.$$

综上分析得到 $\{a_1,a_2,\cdots,a_k\}\cap\{b_1,b_2,\cdots,b_l\}=\{c_1,c_2,\cdots,c_m\}$，即

$$f(a*b)=f(a)\cap f(b).$$

2° 当 $a=0$ 或 $b=0$ 时，$f(a)=\phi$ 或 $f(b)=\phi$，$a\oplus b=b$ 或 $a\oplus b=a$。于是 $f(a\oplus b)=f(b)$ 或 $f(a\oplus b)=f(a)$，最后得到 $f(a\oplus b)=f(a)\cup f(b)$。当 $a\neq 0$ 且 $b\neq 0$ 时，令 $f(a\oplus b)=\{d_1,d_2,\cdots,d_n\}$，$d_1,d_2,\cdots,d_n$ 是小于 $a\oplus b$ 的全部原子。由引理8.3知，对于原子 d_i 和非零元素 a，$d_i\leqslant a$ 或 $d_i\leqslant a'$ 两者必居其一。对于原子 d 和非零元素 b，$d_i\leqslant b$ 或 $d_i\leqslant b'$ 两者必居其一。这里一共有四种可能的组合，其中 $d_i\leqslant a'$ 与 $d_i\leqslant b'$ 不能同时成立(否则由 $d_i\leqslant a'$，$d_i\leqslant b'$ 得到 $d_i\leqslant a'*b'=(a\oplus b)'$，而 $d_i\leqslant a\oplus b$，得出 $d_i\leqslant(a\oplus b)*(a\oplus b)'=0$，这与 d_i 是原子矛盾)。在余下的三种组合中或者 $d_i\leqslant a$ 成立或者 $d_i\leqslant b$，即 $d_i\in\{a_1,a_2,\cdots,a_k\}\cup\{b_1,b_2,\cdots,b_l\}$，最后得到 $\{d_1,d_2,\cdots,d_n\}\subseteq\{a_1,a_2,\cdots,a_k\}\cup\{b_1,b_2,\cdots,b_l\}$。反过来，任取 $x\in\{a_1,a_2,\cdots,a_k\}\cup\{b_1,b_2,\cdots,b_l\}$，显然 $x\leqslant a\leqslant a\oplus b$，$x\leqslant b\leqslant a\oplus b$，于是 $x\in\{d_1,d_2,\cdots,d_n\}$，得到 $\{a_1,a_2,\cdots,a_k\}\cup\{b_1,b_2,\cdots,b_l\}\subseteq\{d_1,d_2,\cdots,d_n\}$。综上分析得出结论 $\{a_1,a_2,\cdots,a_k\}\cup\{b_1,b_2,\cdots,b_l\}=\{d_1,d_2,\cdots,d_n\}$，即

$$f(a\oplus b)=f(a)\cup f(b).$$

3° 当 $a=1$ 时，$f(a')=f(0)=\phi$。而 $\overline{f(a)}=\bar{S}=\phi$，所以

$f(a')=\overline{f(a)}$。当 $a\neq 1$ 时，$f(a')\neq\phi$，这时对于原子 x

$x\in f(a')\Longleftrightarrow x\leqslant a'\Longleftrightarrow x\leqslant a$ 不成立 $\Longleftrightarrow x\notin f(a)\Longleftrightarrow x\in\overline{f(a)}$，

由此得到 $f(a')=\overline{f(a)}$。

由以上讨论知 f 是从 A 到 $\mathscr{P}(S)$ 的同构映射，所以 $\langle A, *, \oplus, ', 0, 1\rangle$ 与 $\langle\mathscr{P}(S), \cap, \cup, ^{-}, \phi, S\rangle$ 两个布尔代数同构。

从以上讨论看出：有限布尔代数中集合 A 的元素个数为 2^n，其中 n 就是布尔格 $\langle A, *, \oplus\rangle$ 中，原子的个数。任何具有 2^n 个元素的布尔代数都是同构的。

8.4.5 布 尔 环

在布尔代数 $\langle A, *, \oplus, ', 0, 1\rangle$ 中，暂时我们只看其中一个二元运算，$\langle A, *\rangle$ 中 $*$ 满足交换律、结合律。对于 A 中任意元素 a 均有 $a*1=a$，所以 1 是 $*$ 运算的单位元。对于元素 a，如果存在 $b\in A$ 使 $a*b=1$，那么 $a=a\oplus(a*b)=a\oplus 1=1$。这表明集合 A 中只有当 $a=1$ 时有逆元，所以 $\langle A, *\rangle$ 构成带 1 半群。$\langle A, \oplus\rangle$ 中 $\oplus$ 满足交换律、结合律。对于 A 中任意元素 a 均有 $a\oplus 0=a$，所以 0 是 $\oplus$ 运算的零元。对于元素 a，如果存在 $b\in A$ 使 $a\oplus b=0$，那么 $a=a*(a\oplus b)=a*0=0$。这表明集合 A 中只有当 $a=0$ 时有负元(为 0)。所以 $\langle A, \oplus\rangle$ 构成带 1 半群。

如果我们看 A 上的两个二元运算，从前面讨论知 $\langle A, *, \oplus\rangle$ 是布尔格，它不能构成环。为此定义 A 上新的二元运算 $+$，$a, b\in A$，

$$a+b=(a*b')\oplus(a'*b)。$$

不难看出 $+$ 运算满足交换律和结合律。0 为零元。由于 $a+a=(a*a')\oplus(a'*a)=0\oplus 0=0$，$a$ 是 a 的负元。从而 $\langle A, +\rangle$ 是交换律。又

$$(a+b)*c=((a'*b)\oplus(a*b'))*c=(a'*b*c)\oplus(a*b'*c),$$

$$(a*c)+(b*c)=((a'\oplus c')*b*c)\oplus(a*c*(b'\oplus c'))$$
$$=(a'*b*c)\oplus(a*b'*c),$$

知 $(a+b)*c=(a*c)+(b*c)$，即 $*$ 对 $+$ 有右分配律。同理可证 $c*(a+b)=(c*a)+(c*b)$，即 $*$ 对 $+$ 有左分配律。

综上知 $\langle A, +, *\rangle$ 是环，我们称它是布尔环。在布尔环中，对任意 A 中元素 a，$a^2=a*a=a$。

反过来，已知 $\langle A, +, \cdot\rangle$ 是布尔环，重新定义。二元运算 $\oplus$ 和一元运算 $'$，$a, b\in A$，

$a\oplus b=a+b+a\cdot b$，

$a'=1+a$，

那么 $\langle A, \cdot, \oplus, ', \cdots\rangle$ 构成布尔代数。该布尔代数的最小元和最大元计算留作习题。

8.4.6 布尔表达式

定义 8.17 布尔代数 $\langle A, *, \oplus, ', 0, 1\rangle$ 上的布尔表达式定义为：

1° A 中任何元素是布尔表达式。

2° 任何变元是布尔表达式。

3° 如果 e_1 和 e_2 是布尔表达式，则 e_1'，$(e_1\oplus e_2)$，$(e_1*e_2$t 均是布尔表达式。

有 n 个不同变元的布尔表达式叫作 n 元布尔表达式，记为 $E(x_1, x_2, \cdots, x_n)$，其中 $x_1, x_2, \cdots, x_n$ 是变元。如果用 A 中元素代替 $x_i(1\leqslant i\leqslant n)$，那么 $E(x_1, x_2, \cdots, x_n)$ 就是 A 中的一个元素。所以 E 是从 A^n 到 A 的映射。如果 $f: A^n\to A$，f 能用 A 上的 n 元布尔表达式表示，那么 f 就叫作 n 元布尔函数。

$\langle\{0, 1\}, \cdot, +, -, 0, 1\rangle$ 是二元布尔代数，任何 n 元开关函数 $f:\{0, 1\}^n\to\{0, 1\}$，我们可以对应函数值为 1 的每个有序 n 数组写出它的小项表达式。由此可知每个开关函数都是布尔函数。可以证明，一般的布尔代数 $\langle A, *, \oplus, ', 0, 1\rangle$ 上的任意布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 可以写成

$$E(x_1, x_2, \cdots, x_n)=\oplus\subset C\delta_1\delta_2\cdots\delta_n*\tilde{x}_1*\tilde{x}_2*\cdots*\tilde{x}_n,$$

其中 $C_{\delta_1\delta_2\cdots\delta_n}\in A$, $\bar{x}_i = x_i$ 或 x_i', $1\leqslant i\leqslant n$.

下面举例说明并非所有的从 A^n 到 A 的映射都是 A 上的布尔函数。取 $A=\{0, 1, 2, 3\}$, $\langle A, *, \oplus, ', 0, 1\rangle$ 的 Hasse 图为图 25,其中 2 与 3 互逆。令 $g: A^2\to A$, g 的定义如右下表。

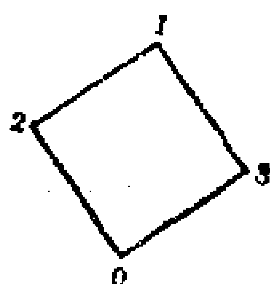


图 25

$g(i,j)$ (i \ j)	0	1	2	3
0	1	0	0	3
1	1	1	0	3
2	2	0	1	1
3	3	0	2	2

如果 g 是布尔函数,应有

$$g(x_1, x_2) = (g(1, 1)*x_1*x_2)\oplus(g(1, 0)*x_1*x_2')$$
$$\oplus(g(0, 1)*x_1'*x_2)\oplus(g(0, 0)*x_1'*x_2')$$
$$=(x_1*x_2)\oplus(x_1*x_2')\oplus(x_1'*x_2').$$

代入 $x_1=x_2=3$,得到

$$g(3, 3)=(3*3)\oplus(3*2)\oplus(2*2)=3\oplus 0\oplus 2=1.$$

而在 g 的定义中 $g(3, 3)=2$,矛盾。故 g 不是布尔函数。

习　　题

1. 令 $R_1=\{x|x\in \mathrm{R}, 0\leqslant x\leqslant 1\}$, $\leqslant$ 是 R_1 上的小于等于关系。证明 $\langle R_1, \leqslant\rangle$ 是格。该格的 $*$, $\oplus$ 运算是什么?

2. $\langle A, \leqslant\rangle$ 是格, a, b, c 是 A 中任意元素,证明:

(1) $a*b=b*a$, $a\oplus b=b\oplus a$.

(2) $a*(a\oplus b)=a$, $a\oplus(a*b)=a$.

3. 证明:在格中,如果 $a\leqslant b$, $c\leqslant d$, 则有 $a*c\leqslant b*d$.

4. 证明:在格中,如果 $a\leqslant b\leqslant c$, 则有

(1) $a\oplus b=b*c$.

(2) $(a*b)\oplus(b*c)=b=(a\oplus b)*(a\oplus c)$.

5. 证明：在格中，

$(a*b)\oplus(c*d)\leqslant(a\oplus c)*(b\oplus d)$,

$(a*b)\oplus(b*c)\oplus(c*a)\leqslant(a\oplus b)*(b\oplus c)*(c\oplus a)$,

6. $\langle A,\leqslant\rangle$ 为格. A 中的元素 $a, b, a<b$. 令

$$B=\{x \mid x\in A \text{ 且 } a\leqslant x\leqslant b\},$$

证明 $\langle B,\leqslant\rangle$ 是格.

7. $\langle A,*,\oplus\rangle$ 是格. A 的元素个数大于 1. 如果该格有最小元 0 和最大元 1，那么它们必然是 A 的不同元素.

8. 设 $S=\{1,3,5,15,25,75\}$，$\langle S,|\rangle$ 是格. 请列中 S 有补元的元素并写出它们的补元.

9. 在具有两个或更多个元素的格里，不会有元素是它自身的补.

10. 具有三个或更多元素的线性序集不是有补格.

11. 5阶格中哪些是分配格？

12. 证明：格是分配格当且仅当对任意元素 a, b, c，$(a*b)\oplus(b*c)\oplus(c*a)=(a\oplus b)*(b\oplus c)*(c\oplus a)$.

13. 证明：在有补分配格中

(1) $a\leqslant b \Leftrightarrow a*b'=0$.

(2) $b'\leqslant a' \Leftrightarrow a'\oplus b=1$.

14. f 是从集合 A 到集合 B 的映射. 令 $S=\{f(c) \mid c\in \mathscr{P}(A)\}$，证明 $\{S,\subseteq\}$ 是 $\{\mathscr{P}(B),\subseteq\}$ 的子格.

15. $\langle A,\leqslant\rangle$ 是分配格. a, b 是 A 中元素，$a<b$. 令 $B=\{x \mid x\in A, a\leqslant x\leqslant b\}$. 证明 $f(x)=(x\oplus a)*b$ 是从 A 到 B 的同态映射.

16. $\langle S,\leqslant\rangle$ 是模格. a, b 是 S 的元素. 令

$$X=\{x \mid x\in S,\ a*b\leqslant x\leqslant a\},$$
$$Y=\{y \mid y\in S,\ b\leqslant y\leqslant a\oplus b\},$$

$f(x)=x\oplus b$，证明 f 是从 X 到 Y 的同构映射.

17. 在布尔代数 $\langle A, *, \oplus, ', 0, 1\rangle$ 中，对于 A 中任意元素 a, b.

(1) $a\oplus(a'*b)=a\oplus b$.

(2) $a*(a'\oplus b)=a*b$.

18. 证明：在布尔代数中 $x\leqslant y \Leftrightarrow y'\leqslant x'$.

19. $\langle A_1, *, \oplus, ', 0, 1\rangle$ 与 $\langle A_2, \wedge, \vee, -, \tilde{0}, \tilde{1}\rangle$ 是两个布尔代数. 在集合 $A_1\times A_2$ 上定义运算 ^{0}, $\tilde{*}$, $\tilde{\oplus}$:

$(a_1, a_2)^0=(a'_1, \bar{a}_2)$,

$(a_1, a_2)\tilde{*}(b_1, b_2)=(a_1*b_1, a_2\wedge b_2)$,

$(a_1, a_2)\tilde{\oplus}(b_1, b_2)=(a_1\oplus b_1, a_2\vee b_2)$.

证明 $\langle A_1\times A_2, \tilde{*}, \tilde{\oplus}, {}^\circ, (0, \tilde{0}), (1, \tilde{1})\rangle$ 是布尔代数。

20. A, B 是两个非交集合. 任取 $S\subseteq A, T\subseteq B$, 令 $f(S\cup T)=(S, T)$. 证明: f 是 $\langle \mathscr{P}(A\cup B), \subseteq\rangle$ 到 $\langle \mathscr{P}(A)\times\mathscr{P}(B), \subseteq\rangle$ 两个布尔代数间的同构映射。

21. 找出 8 元布尔代数的所有子代数。

22. $\langle\{1, 2, 3, 4, 6, 12\}, |\rangle$ 及 $\langle\{1, 2, 3, 4, 6, 8, 12, 24\}, |\rangle$ 是布尔代数吗?

23. 若 $a, b_1, b_2, \cdots, b_r$ 是布尔代数 $\langle A, *, \oplus, ', 0, 1\rangle$ 的原子, 证明

$a\leqslant(b_1\oplus b_2\oplus\cdots\oplus b_r)\Leftrightarrow$ 存在 i, 使 $a=b_i, 1\leqslant i\leqslant r$.

24. 若 $b_1, b_2, \cdots, b_n$ 是有限布尔代数中的所有原子, 证明

$y=0\Leftrightarrow\forall i, y*b_i=0, 1\leqslant i\leqslant n$.

25. $\langle A, +, \cdot\rangle$ 是布尔环. 在 A 上定义运算 $\oplus, '$:

$$a\oplus b=a+b+a\cdot b,$$

$$a'=1+a,$$

证明 $\langle A, \cdot, \oplus, '\rangle$ 是布尔代数。